LANDTAG DES SAARLANDES

12. Wahlperiode **Drucksache 12/367**

14.03.2001

ACHTZEHNTER BERICHT

über die Tätigkeit des Landesbeauftragten für Datenschutz

gemäß § 27 des Saarländischen Gesetzes

zum Schutz personenbezogener Daten

Berichtszeitraum: 1999 und 2000

Ausgegeben:

Inhaltsverzeichnis

1 Allgemeines

Es mag widersprüchlich erscheinen, wenn Menschen, die – freiwillig – ihr Innerstes vor laufender Kamera ausbreiten, die Verarbeitung ihrer personenbezogenen Daten durch Andere nicht hinnehmen wollen. Nur scheinbar ist dies jedoch ein Widerspruch. Denn jemand kann sehr wohl bereit sein, etwas freiwillig über sich preiszugeben, wenn er (oder sie) selbst bestimmt, was die anderen wissen sollen, und wenn er (oder sie) abschätzen kann, wie weiter mit den Informationen umgegangen wird. Dagegen muss niemand akzeptieren, dass seine Daten von öffentlichen Stellen oder geschäftsmäßig von nichtöffentlichen Stellen verarbeitet werden, ohne dass die Einwilligung hierfür gegeben wurde oder eine gesetzliche Rechtfertigung hierfür vorliegt.

Diese scheinbaren Widersprüche müssen wir auch gesamtgesellschaftlich zu lösen versuchen, wenn der Ausgleich zwischen Datenschutz und anderen Interessen zu finden ist. Hier ist es ebenfalls keineswegs so, dass eindimensional die Privatsphäre des Einzelnen den Belangen der Allgemeinheit gegenübersteht. Informationelle Selbstbestimmung Einzelner ist Grundbedingung auch der demokratischen Ordnung insgesamt. „Betroffene“ und „Begünstigte“ sind oft identisch, wenn es um Garantie von Sicherheit durch Videoüberwachung, um Ausschluss von Leistungsmissbrauch oder Steuerbetrug durch Datenabgleich, um Vorsorge gegen Krankheiten oder Beweiserleichterung durch Genomanalyse geht. Wie der Wert von Gesundheit oft erst bei Erkrankung deutlich wird, sieht man den Verlust der Privatheit vielfach erst im Konfliktfall.

Dafür zu sorgen, dass es hierfür nicht zu spät ist, ist Ziel des Datenschutzes. Dies ist Aufgabe der Gesetzgebung und der Stellen selbst, die mit personenbezogenen Daten umgehen (müssen). Den Kontrollstellen wie dem Landesbeauftragten für Datenschutz ist auferlegt, sorgsam darauf zu achten, dass dies auch geschieht, Hilfen hierfür zu geben und den Betroffenen bei der Wahrnehmung seiner Rechte zur Seite zu stehen. Eine Erledigung dieser Daueraufgabe ist nicht in Sicht.

Datenschutz bedeutet keineswegs, generell die Verarbeitung in Zweifel zu ziehen oder gar abzulehnen, auch nicht den Wechsel von konventionellem Umgang zu automatisierten Verfahren. Im Gegenteil kann gerade das gut organisierte EDV-Verfahren besser dem Schutz des Rechts auf informationelle Selbstbestimmung gerecht werden als der überkommene Umgang in hergebrachten Bahnen, wenn man diese nicht laufend auf ihre Schwachstellen überprüft. Selbstverständlich ist es meine Aufgabe, Regelungen, Verfahren und tatsächliche Handhabung in den öffentlichen Stelle argwöhnisch zu betrachten und auf Fehler aufmerksam zu machen. Wie meine

Kollegen sehe ich mich hierbei aber nicht als Verhinderer, sondern als Helfer der Administratoren und Anwender in den öffentlichen Stellen.

In den Berichtszeitraum fiel mit Beginn der neuen Legislaturperiode des Landtags auch der Wechsel in der Regierungsverantwortung auf Landesebene. Mit einzelnen Mitgliedern der Landesregierung habe ich grundsätzliche Fragen in einem ersten Gespräch erörtern und mein Bemühen darstellen können, bei meiner Tätigkeit den präventiven Aspekt in den Vordergrund zu stellen. Dies bedingt natürlich, dass meine Dienststelle frühzeitig über Vorhaben unterrichtet wird, um rechtzeitig auf mögliche Schwächen hinweisen und Vorschläge unterbreiten zu können. Erfreulicherweise wächst diese Bereitschaft hierzu in den Verwaltungen selbst.

In der Regierungserklärung des neugewählten Ministerpräsidenten kam der Datenschutz als Schwerpunkt der künftigen Politik nicht vor, und auch in der Normsetzung des Landtags in der neuen Wahlperiode waren – vor allem mit der Novelle des Polizeigesetzes – insoweit eher Rückschritte als Verbesserungen zu verzeichnen. Ich habe die Hoffnung, dass bei den noch anstehenden weiteren Vorhaben die Gewichte anders verteilt werden. Wesentlich wird vor allem sein, dass mit Überarbeitung des Datenschutzgesetzes selbst ein Schritt nach vorn getan wird.

Wie immer gibt der vorliegende Tätigkeitsbericht nur einen Ausschnitt aus der Beratungs- und Kontrollarbeit meiner Dienststelle. An der Zielsetzung, stärker vorbeugend mit beispielhaften Hilfen und Einzelberatungen zur Verbesserung beizutragen als mit - gar spektakulär herausgehobenem – Vorhalten von Datenschutzverstößen, habe ich festgehalten. Gerade für die immer stärker auch von den Stellen selbst nachgefragten Hilfen im engeren IT-Bereich stoße ich aber mit unserer geringen Personalausstattung an bzw. über meine Grenzen. Abhilfe ist dringend nötig.

Bei der Kontrolltätigkeit stelle ich selbstverständlich in der Regel fest, dass die geprüften Stellen ordnungsgemäß mit den Daten umgehen, ohne dass dies in meinen Prüfungsbemerkungen oder in diesem Bericht zum Ausdruck kommt. Erwähnenswert sind meist nur Unregelmäßigkeiten. Die Veröffentlichung von „Mängeln“ und von Abhilfemöglichkeiten dient aber zugleich Anwendern in anderen Bereichen, solche Fehler zu vermeiden, sowie den Betroffenen als Hinweis für das Wahrnehmen ihrer Rechte. Mit der Vorlage des Tätigkeitsberichts erfülle ich deshalb nicht nur meine gesetzliche Pflicht, Rechenschaft abzulegen über das Handeln einer Dienststelle, die mit guten Gründen nicht in die übliche parlamentarische Verantwortung eingebunden ist.

Es ist im wesentlichen das Engagement meiner Mitarbeiter, dem ich meine Tätigkeit zu verdanken habe. Hilfreich ist der Kontakt mit den Kollegen im

Bund und den übrigen Ländern, vor allem in den Fach-Arbeitskreisen, die oft vergleichbar auftretende Probleme abstimmen und meist gemeinsame Positionen erarbeiten. In einer Reihe von Einzelfragen haben die Datenschutzbeauftragten sich mit Entschließungen an die gesetzgebenden Organe, aber auch an Industrie und Verfahrensentwickler gewandt; sie sind im Anhang abgedruckt. Den zuständigen Ressorts der Landesregierung habe ich sie jeweils zugeleitet.

Als gemeinsame Aktivität möchte ich auch ein Projekt erwähnen, das vom schleswig-holsteinischen Kollegen initiiert und unter Mitwirkung von verschiedenen Datenkontrollstellen auch im Ausland auf den Weg gebracht worden ist. Mit einem „Virtuellen Datenschutzbüro (vDSB)“ soll – über das Internet – vor allem eine Kommunikationsplattform untereinander, der Meinungsaustausch mit Experten und die Möglichkeit für Bürger entstehen, auf häufig gestellte Fragen kompetent Antwort zu erhalten. Gerade die grenzübergreifende Natur des Internet lässt eine gemeinsame Tätigkeit und die Nutzung gerade dieser Technik hierfür sinnvoll erscheinen; die engen personellen Grenzen meiner Dienststelle haben mir indes eine intensive Mitwirkung bisher verwehrt.

Natürlich kann dieses Angebot meine originäre Zuständigkeit für den Datenschutz bei den öffentlichen Stellen im Saarland nicht ersetzen, auf die ich meine Kapazitäten konzentrieren muss. Ich bin weiterhin bemüht, für eigene Informationen und für die Kontaktaufnahme mein Internet-Angebot (**www.lfd.saarland.de**) aufrecht zu erhalten und auszubauen, mit dem die öffentlichen Stellen wie Bürgerinnen und Bürger auf einschlägige Rechtsvorschriften, Orientierungshilfen und Materialien für Anwender und auch auf die Tätigkeitsberichte zugreifen können.

2 Technisch-organisatorischer Datenschutz

Sowohl bei der Datenverarbeitung in konventioneller Art als auch besonders bei Nutzung der EDV gehören technisch-organisatorische Vorkehrungen bei den öffentlichen Stellen unabdingbar zum notwendigen Schutz des Rechts auf informationelle Selbstbestimmung. Ihr Vorhandensein und vor allem ihre Beachtung ist selbstverständlich Gegenstand meiner Kontrolltätigkeit in allen Sachbereichen. In diesem vorangestellten Abschnitt möchte ich gesondert auf diese Schutzmaßnahmen hinweisen und dabei den beratenden Aspekt meiner Tätigkeit betonen.

2.1 IT-Dienstanweisungen in den Kommunen

In den beiden Berichtsjahren habe ich mich verstärkt mit der Erfüllung datenschutzrechtlicher Anforderungen bei Kreisen, Städten und Gemeinden befasst. Ein Schwerpunkt lag hierbei auf der Inkraftsetzung von Dienstan-

weisungen für den Einsatz der Informationstechnik, die als wichtigste organisatorische Maßnahme nach § 11 SDSG zentrale Vorgaben für die Realisierung von Datenschutz und Datensicherheit in der Gesamtorganisation und bei den einzelnen Verfahren gibt. In vielen Kommunen stand die Ablösung der veralteten Anlagen bevor; ich wollte mithelfen, dass neue Einrichtungen und Verfahren mehr als bisher den datenschutzrechtlichen Bestimmungen entsprechen. Meine früheren Hinweise auf die geltenden gesetzlichen Bestimmungen hatten äußerst geringe Resonanz gefunden. Insofern hoffte ich, dass die Umsetzung eher durch Eigenverpflichtung im Rahmen einer Dienstanweisung gelingen könne.

Zur Erleichterung für die Bearbeiter hatte ich schon 1995 Muster-Dienstanweisungen mit einer Gemeinde und einem Landkreis erarbeitet. Diese wurde aber von vielen Dienststellen nur als Posteingang registriert und nicht in praktische Ergebnisse umgesetzt. Möglicherweise scheute man auf Grund der allgemein schlechten Personallage den Aufwand zur Regelung und letztendlich auch die daraus folgenden Konsequenzen. Denn wenn auch einsehbar ist, dass Datenverarbeitung erst mit transparent festgelegtem Verfahren eingeführt und verantwortbar eingesetzt werden kann, dann aber sowohl höhere Sicherheit und Zuverlässigkeit bietet als auch den gesetzlichen Anforderungen entspricht, wollen viele nicht akzeptieren, dass hierfür ein gewisser organisatorischer und personeller Aufwand nötig ist.

Alle Kreise und der Stadtverband und fast alle Gemeinden haben inzwischen eine Dienstanweisung erarbeitet, mit mir abgestimmt und in Kraft gesetzt. Wenige Gemeinden und ein Landkreis mussten hierzu erst mit Hilfe der Kommunalaufsicht überzeugt werden. Die wenigen, aus nachvollziehbaren Gründen noch ausstehenden Gemeinden haben sich ebenfalls zum Abschluss bereit erklärt, und ich gehe davon aus, dass diese Aktivitäten im Jahr 2001 abgeschlossen werden können. Dann werden überall im kommunalen Bereich klare Regelungen bei der Datenverarbeitung im Interesse der Dienststellen, aber auch der Mitarbeiter gelten; damit wird auch eine Umsetzung der geltenden datenschutzrechtlichen Regelungen (z. B. Beteiligung des LfD, technische und organisatorische Maßnahmen, Freigabe der Verfahren, Dateibeschreibung, Meldung zum Dateienregister) erleichtert.

2.2 IT-Sicherheitskonzept des Ministeriums für Frauen, Arbeit, Gesundheit und Soziales

Eigentlich ist selbstverständliche Voraussetzung jeden verantwortbaren EDV-Einsatzes, dass zuvor die hiermit verbundenen Risiken festgestellt und angemessene Schutzmaßnahmen festgelegt werden. In der Praxis ist dies aber oft nicht nachvollziehbar belegt, weil auch diese Vorarbeit Aufwand bereitet; dass es notwendig ist, wird aber nicht bestritten. Die saarländische Landesverwaltung hatte sich 1997 zum Ziel gesetzt, den sicheren und da-

tenschutzgerechten Einsatz von Verfahren auf Basis einer Risikoanalyse und eines Sicherheitskonzepts zu gestalten.

Das Ministerium für Frauen, Arbeit, Gesundheit und Soziales (MiFAGS) unternahm die Herkules-Arbeit, einmal für ein gesamtes Ministerium und alle unterschiedlichen Anwendungsbereiche ein solches Sicherheitskonzept zu erstellen. Wie in der IT-Sicherheitsrichtlinie vorgesehen, wurde ein Sicherheitsmanagement eingesetzt, dem die entscheidenden Stellen des Hauses angehörten. Zuerst wurde eine Bestandsaufnahme der eingesetzten Informationstechnik und der betriebenen Verfahren vorgenommen. In einem zweiten Schritt wurden dann die Sensibilität der zu verarbeitenden personenbezogenen Daten bewertet, eine Beschreibung der mit den unterschiedlichen Betriebsformen verbundenen Risiken erstellt und aus dem IT-Grundschutzhandbuch jeweils geeignete Maßnahmen entnommen, um eine angemessene Sicherheit gewährleisten zu können. Der gesamte Prozess lief in enger Abstimmung mit meiner Dienststelle.

Das erarbeitete Konzept diente dem Ministerium selbst als Grundlage für die Umsetzung der erarbeiteten Maßnahmen, für weitere Konzepte im nachgeordneten Bereich (z. B. Landesamt für Arbeitssicherheit, Immissionsschutz und Gesundheit und die IT-Einführung bei den Landesarbeitsgerichten) und führte zu einer abgerundeten hausinternen IT-Dienstanweisung. Das Sicherheitskonzept wurde nach seiner Fertigstellung den anderen obersten Landesbehörden als Muster zur Verfügung gestellt. Ich hoffe, dass die übrigen Ressorts diese Materialien nutzen, um daraus ein eigenes Konzept abzuleiten; die umfangreichen Vorarbeiten des MiFAGS machen dies mit relativ geringem Aufwand möglich.

2.3 Online-Kfz-Zulassung im Landkreis Saarlouis

In vergleichbarer Weise habe ich versucht, auf Landkreisebene an der Entwicklung eines beispielhaften Verfahrens mitzuwirken.

Der Landrat des Kreises Saarlouis beabsichtigte, die Abwicklung der Kraftfahrzeugzulassung durch die Nutzung von Internet-Technologien wesentlich zu verbessern und zu erleichtern; das Zulassungsverfahren sollte effizienter, schneller, zeitunabhängiger und kundenfreundlicher gestaltet werden. Dazu sollten Zulassungsdaten von den Händlern und Zulassungsdiensten über das Internet zur Zulassungsstelle übermittelt werden, die dann die Daten ohne eigene Datenerfassung in ihr Verfahren übernehmen und den zuliefernden Stellen bzw. den Schilderprägern das zugeteilte Kennzeichen und die Fertigstellung des Vorgangs mitteilen wollte. Für den Bürger sollte ergänzend die Möglichkeit eröffnet werden, Wunschkennzeichen über das Internet zu reservieren. Die gesamten Internet-Aktivitäten sollten über einen privaten Dienstleister datenschutzgerecht abgewickelt werden; die Zulassungsstelle sollte natürlich jederzeit Herr des Verfahrens und der Daten

sein, und ein Durchgriff auf die Rechnersysteme des Kreises und damit eine Gefährdung der Verfahren und Daten musste ausgeschlossen bleiben.

In enger Abstimmung zwischen Kreisverwaltung, privatem Auftragnehmer und LfD gelang es, das beabsichtigte Projekt datenschutzgerecht bis zum Echteinsatz zu entwickeln. Auf der Basis der IT-Sicherheitsrichtlinie des Saarlandes wurden eine Risikoanalyse und ein IT-Sicherheitskonzept entwickelt; vor der Freigabe des Verfahrens waren die entscheidenden Maßnahmen umgesetzt. Speziell dafür geschulte Mitarbeiter der Händler und Zulassungsdienste greifen nach gesicherter Authentifikation auf den Web-Server des Dienstleisters zu und legen dort die Zulassungsdaten ab. Zusätzlich werden die für die Abwicklung notwendigen Papierunterlagen im Nachttresor der Zulassungsstelle eingeworfen. Die Zulassungsstelle übernimmt diese Daten zu planbaren Zeitpunkten vom Server, wickelt das Zulassungsverfahren nach Sichtkontrolle der elektronischen Daten und Papierunterlagen im hausintern abgeschotteten Online-Verfahren der Zulassungsstelle ab und übermittelt die Kennzeichen an die Händler, Zulassungsdienste und Schildermacher zur weiteren Abwicklung. Die Datenübertragung über das Internet ist durch eine SSL-Verschlüsselung gesichert. Ein Durchgriff auf die Netze, Rechner und Daten der Kreisverwaltung wird zusätzlich durch eine Firewall verhindert. Alle innerhalb des Online-Verfahrens auftretenden Zugriffe werden protokolliert und zeitnah ausgewertet. Für die Auftragsdatenverarbeitung des privaten Dienstleisters wurde auch ein datenschutzgerechter Dienstleistungsvertrag konzipiert und in Kraft gesetzt. Die hier modellhaft entwickelte Anwendung soll bundesweit auch in anderen Zulassungsstellen zum Einsatz kommen. Die Risikoanalyse und das Sicherheitskonzept wurden den Datenschutzbeauftragten des Bundes und der Länder zur Verfügung gestellt.

2.4 Muster-Sicherheitskonzept zum Einsatz von Care beim Saarpfalzkreis

Der Saarpfalzkreis beabsichtigte, das Verfahren CARE in seinem Sozialamt als Netzwerklösung zur Berechnung und Zahlbarmachung der Sozialhilfe sowie entsprechender Leistungen für Asylbewerber einzusetzen. Das Verfahren sollte auch die Erstellung der amtlichen Sozialhilfe-Statistik unterstützen.

Das Verfahren CARE wurde bisher bundesweit und im Saarland auf Einzelarbeitsplätzen eingesetzt; soweit es im Netz erfolgte, gab es jedoch keine klare Beschreibung, inwieweit dies datenschutzrechtlichen Anforderungen entspricht. Die Kreisverwaltung, insbesondere das Sozialamt erklärte sich bereit, auf Basis der IT-Sicherheitsrichtlinie des Saarlandes eine komplette Risikoanalyse und ein Sicherheitskonzept unter Anwendung des IT-Grund-

schutzhandbuchs des BSI für den geplanten Einsatz zu erstellen und diese Ergebnisse als Muster zur Verfügung zu stellen.

Auch hier war meine Dienststelle zu einem frühen Zeitpunkt an der Konzeption und Durchführung beteiligt. Dabei wurden die Sensibilität der zu verarbeitenden personenbezogenen Daten bewertet, eine Beschreibung der mit dem Netzbetrieb verbundenen Risiken erstellt und aus dem IT-Grundschutzhandbuch geeignete Maßnahmen entnommen, um eine angemessene Sicherheit herstellen zu können. In Abstimmung mit dem Software-Ersteller wurde auch eine Muster-Meldung zum Dateienregister entwickelt, so dass in Zukunft allen öffentlichen Stellen der datenschutzgerechte Einsatz, die Freigabe des Verfahrens und die Meldung zum Dateienregister wesentlich erleichtert und für den LfD der Aufwand für eine Beteiligung vor der Einführung eines solchen Verfahrens deutlich reduziert wird. Zusätzlich wurde auch noch eine datenschutzgerechte Vertragsgestaltung unter Berücksichtigung der BVB-Vertragsmuster entwickelt.

2.5 Neuausschreibung des Landesdatennetzes und Verschlüsselung

1998 hatte der Ministerrat ein Gutachten in Auftrag gegeben, das die Organisation der Sprach- und Datenübertragung insbesondere für die Behörden und Einrichtungen des Landes untersuchen sollte. Erfreulicherweise hatte mich die Landesregierung schon in die Vertragsgestaltung und damit die Festlegung des Arbeitsauftrages einbezogen. So konnte ich schon im Vorfeld auf die Notwendigkeit einer Basis-Verschlüsselung der Datenübertragung hinweisen.

Das dann im Mai 1999 vorgelegte Gutachten enthielt unter anderem Vorschläge zur Zusammenfassung der bestehenden Datennetze unter virtueller Aufsplittung für notwendige Teilnetze und zentraler Administration. Die Gutachter hatten die von mir angeregte Verschlüsselung berücksichtigt. Darüber hinaus enthielt das Gutachten die Empfehlung, über dieses Datennetz auch die Telefonie abzuwickeln und dazu alternativ die Administration der Haupt- und Nebenstellenanlagen mit Hilfe des Centrex-Dienstes ebenfalls zu zentralisieren oder aus Kostengründen möglicherweise sogar zu privatisieren.

Insbesondere mit Blick auf die mögliche Privatisierung der Administration mit ihren weitrechenden Kontroll- und Kenntnisnahmemöglichkeiten für hochkritische Daten und Telefongespräche habe ich eine Risikoanalyse und ein Sicherheitskonzept gefordert, auf Basis derer die Entscheidung zu Zentralisierung und Privatisierung getroffen werden sollte. Ergänzend habe ich auf die Sicherheitsmaßnahmen verwiesen, die schon bei der Realisierung der gemeinsamen TK-Anlage der Landesverwaltung mit mir abgestimmt wurden. Hierzu gehören insbesondere eine Absicherung aktivierter Leistungsmerkmale bei Installation und Wartung gegen Manipulation, eine sichere Administration der individuellen Berechtigungen im Rahmen aktivierter Lei-

stungsmerkmale und die Vermeidung von Fernwartung bzw. Fernadministration.

Das Projekt ist inzwischen bis zu einer europaweiten Ausschreibung gediehen und enthält auch den wichtigen Aspekt einer Basis-Verschlüsselung der Datenübertragung. Ich werde darauf achten, dass bei der Umsetzung Datenschutz- und damit zugleich Sicherheitsaspekte nicht unter Kostenaspekten vernachlässigt werden.

2.6 Organisationsvorschriften in der Landesverwaltung

Positiv begleite ich das Anliegen der Landesregierung, die verstreut vorhandenen untergesetzlichen Vorschriften zu durchforsten, und, wo für sie kein Bedarf mehr besteht, aufzuheben. Der Ministerrat hat hierfür ein stringentes Verfahren gewählt, nach dem – zeitlich gestuft – alte Erlasse und Regelungen automatisch aufgehoben werden, wenn deren generelle Weitergeltung oder ein Hinausschieben der Außerkrafttretung nicht von einer Arbeitsgruppe oder dem Kabinett beschlossen wird.

Betroffen sind selbstverständlich auch Bestimmungen, die sich auf die Verarbeitung personenbezogener Daten beziehen. Sicher gibt es hier ebenfalls entbehrliche und überholte Bestimmungen, die faktisch ohnehin vielfach nicht angewandt werden. Mit einer Konzentration auf die wirklich (noch) relevanten Vorschriften erhöht sich die Transparenz für Sachbearbeiter und für Betroffene und vor allem die Wahrscheinlichkeit ihrer Beachtung.

Der radikale Ansatz zur „Entrümpelung“ verführt indes dazu, als Erfolg schon den Wegfall einer möglichst hohen Zahl von Vorschriften zu werten. Das Einstampfen von nach Gewicht bemessenen Papieren kann nicht oberstes Ziel einer geordneten Verwaltung sein, die auf Gesetzmäßigkeit und korrekte Amtsführung verpflichtet ist. Manchmal ist sachlich geradezu unabdingbar, Detailfestlegungen auch genereller Art innerhalb der Verwaltung zu treffen, auf die die gesetzliche Norm verzichten muss.

2.6.1 Überarbeitung der IT-Organisationsvorschriften

Da vom automatischen Wegfall aus datenschutzrechtlicher Sicht sehr wichtige Verwaltungsvorschriften, wie z. B. die ADV-Projektrichtlinien betroffen waren, habe ich schon 1999 in Abstimmung mit dem Rechnungshof eine Übersicht über alle geltenden Gesetze, Organisationsvorschriften, Ministerratsbeschlüsse und Empfehlungen des LfD zum Bereich Informationstechnik erstellt und die Bildung einer Arbeitsgruppe angeregt, die sich der Außerkraftsetzung bzw. Weitergeltung oder Überarbeitung annehmen sollte. Zu den wichtigsten Regelungen - den ADV-Projektrichtlinien - hatte ich schon relativ früh auf Grund von Abschlusstests zu neuen Verfahren, bei denen deutlich wurde, dass die inzwischen in Teilen veralteten Vorschriften nicht

mehr passten, Formulierungsvorschläge zur Überarbeitung vorgelegt; sie wurden aber bisher noch nicht berücksichtigt. Rechtzeitig zum Jahresende 2000 trat dann die Unterarbeitsgruppe des IK-Ausschusses zur „Modernisierung der IT-Richtlinien und -Standards“ zusammen, beantragte eine vorübergehende Weitergeltung der einschlägigen Vorschriften und einigte sich auf konkrete Überarbeitungstermine im Jahr 2001. Ich werde bei der Überarbeitung der Vorschriften dazu beitragen, dass die datenschutzrechtlichen Belange in angemessener Form zur Geltung kommen.

2.6.2 Gemeinsame Geschäftsordnung für alle obersten Landesbehörden

Ich hatte auch die Möglichkeit, bei der Vorbereitung einer „Gemeinsamen Geschäftsordnung (GGO) für die obersten Landesbehörden“ mitzuhelfen, dass - diese jetzt einheitlichen, für alle obersten Landesbehörden und die Vertretung des Saarlandes beim Bund geltenden - Regelungen, die auch als Orientierungshilfe für den nachgeordneten Bereich gedacht sind, datenschutzrechtliche Aspekte berücksichtigen. Besonders zu erwähnen sind dabei eine vom Ausschuss für Informationstechnologie- und Kommunikation erarbeitete Regelung zur Internet- und eMail-Nutzung, eine Klarstellung zur persönlichen Adressierung von Post und eine datenschutzgerechte Regelung für die Begleitung behördlichen Handelns durch Medienvertreter. Auch gelang es, wichtige Aspekte einer datenschutzgemäßen Behandlung von Telefaxen zu ergänzen, so dass die bisher üblichen, eigenständigen Telefax-Dienstanweisungen entbehrlich sind.

2.7 Internet-Angebot der Landesregierung, X500-Verzeichnisse, eMail-Verschlüsselung

Die Landesregierung unterhält ein Internet-Angebot, mit dem sie Informationen der Allgemeinheit zugänglich macht und Kontaktmöglichkeiten eröffnet. Es wurde im Berichtsjahr 2000 gestrafft und vereinheitlicht; mehr als bisher können die Ressorts jetzt selbst mit Hilfe eines Redaktionssystems den ihnen zugeordneten Bereich unter einheitlichen Rahmenbedingungen gestalten. Ich wurde an der Änderung beteiligt.

Ein wichtiger Aspekt war die Frage, in welchem Umfang personenbezogene Daten in den Darstellungen auftreten können. Insbesondere war festzulegen, inwieweit Geschäftsverteilungspläne und Telefonverzeichnisse zugreifbar sein können. Hierzu hatte ich in meinem Merkblatt für die Internet-Nutzung durch öffentliche Stellen bereits früher Position bezogen.

Mit der Landesregierung wurde dahingehend Übereinstimmung erzielt, dass von außen zugreifbare Seiten möglichst mit funktionalen Bezeichnungen und eMail-Adressen bestückt sind. Ausnahmen von dieser Regel wurden dann akzeptiert, wenn bestimmte Personen durch ihr öffentliches Amt (z. B.

Minister, Staatssekretär, Abteilungsleiter) oder als besonderer Ansprechpartner (z. B. persönlicher Referent, Pressebeauftragter, Bürgerbeauftragter) auch persönlich in Erscheinung treten können bzw. müssen.

Im nur für die Landesverwaltung intern zugreifbaren Intranet können hingegen alle jetzt auch schon über Papierlisten verteilten Geschäftsverteilungspläne und Telefonverzeichnisse präsentiert werden und damit für aktuellere Information im Dienstbetrieb sorgen. Die Rechtsgrundlage für diese Präsentation stellt § 29 SDSG dar. Bei zunehmender Verlagerung von Schriftverkehr in Papierform auf eMail-Technik können diese Verzeichnisse dann auch den öffentlichen Schlüssel für ein leistungsfähiges Verschlüsselungsverfahren enthalten, das dann zur Absicherung der meist über unsichere Leitungen versandten und unter Umständen höchst sensiblen Informationen genutzt werden kann. Mitte des Jahres 2000 wurde hierzu in der Landesverwaltung ein Testbetrieb mit Hilfe des Verschlüsselungsprogramms PGP eröffnet, um erste Erfahrungen mit einer asymmetrischen Verschlüsselung zu gewinnen.

2.8 Änderung der Gleitzeiterfassung in der Landesverwaltung

Aufgrund einer Neufassung der Verordnung über die Arbeitszeit der Beamtinnen und Beamten vom 18. 5. 99 mussten die geltenden Gleitzeitregelungen innerhalb 3 Monaten überarbeitet werden; in Teilbereichen wurde die Gleitzeit neu eingeführt. Da die Bearbeitung fast überall unter Einsatz der EDV erfolgt, für die es bereits eingeführte Verfahren gab, mussten diese angepasst werden.

Dazu wurde das entsprechende Projekt beim Ministerium für Bildung, Kultur und Wissenschaft aus datenschutzrechtlicher Sicht modellhaft begleitet, wobei als Grundlage die schon abgestimmten Regelungen des Ministeriums für Finanzen hinzugezogen wurden. Mit dem Hochbauamt wurden auch die Anforderungen für die Ausschreibung der Erfassungstechnik besprochen. Mit dem betroffenen Ministerium konnten die technischen und organisatorischen Maßnahmen zum Einsatz der Verfahren befriedigend konzipiert und umgesetzt werden. Nachdem letztendlich auch noch eine Dienstvereinbarung mit der Personalvertretung abgeschlossen war, dienten die Unterlagen als Muster für die weitere Einführung der Gleitzeit in anderen Dienststellen.

2.9 Muster-Vertrag zur Auftragsdatenverarbeitung

Bei der Kontrolle öffentlicher Stellen muss ich immer wieder feststellen, dass bei Verträgen zur Auftragsdatenverarbeitung aus datenschutzrechtlicher Sicht unzureichende Muster-Formulare der Auftragsnehmer zu Grunde gelegt werden. Erfahrungsgemäß tragen diese Formulare überwiegend den Interessen der Auftragnehmer Rechnung und berücksichtigen zuwenig die

Interessen bzw. Anforderungen des Auftraggebers, der doch die datenschutzrechtliche Verantwortung zu tragen hat.

So findet sich in den Verträgen in der Regel keine Formulierung, die den Bestimmungen des § 5 SDSG Rechnung trägt, nach denen der Auftragnehmer, sofern das SDSG auf ihn keine Anwendung findet, „die Bestimmungen dieses Gesetzes befolgt und sich der Kontrolle des Landesbeauftragten für Datenschutz unterwirft“. Darüber erlauben die Muster-Verträge häufig ausdrücklich, dass sich der Auftragnehmer bei der Ausführung auch ohne Zustimmung des Auftraggebers der Mithilfe Dritter bedienen kann. Unter solchen Umständen kann der Auftraggeber nicht mehr sicher sein, dass die Verarbeitung seiner Daten nur nach seinen Weisungen erfolgt.

Zur Lösung dieser Problematik hatte ich in der Vergangenheit auf die Besonderen Vertragsbedingungen BVB (z. B. Besondere Vertragsbestimmungen für die Überlassung - GMBl 1978, S. 235 -, Wartung -GMBl 1974, S. 721 - und Pflege - GMBl 1980, S. 193) als Anhalt für geeignete Formulierungen verwiesen. Ende 2000 wurden die „Ergänzenden Vertragsbedingungen EVB-IT“ als Ersatz für die BVB eingeführt. Diese Verträge sollten, um den Anforderungen des § 5 Abs. 3 SDSG Rechnung zu tragen, ausdrücklich um eine Bestimmung ergänzt werden, die etwa folgenden Inhalt hat: „Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Der Auftragnehmer befolgt die Bestimmungen des SDSG und unterwirft sich bezüglich der Auftragsdatenverarbeitung der Kontrolle des Landesbeauftragten für Datenschutz. Unterauftragsverhältnisse bedürfen der Zustimmung des Auftraggebers.“

Um den öffentliche Stellen die Praxis zu erleichtern, habe ich einen Muster-Vertragsentwurf meines hessischen Kollegen übernommen, an saarländische Gegebenheiten angepasst und zur Anwendung empfohlen. Dieser Vorschlag kann aus meinem Internet-Angebot abgerufen werden.

2.10 „Der sichere Arbeitsplatz-PC“

Explosionsartig sich weltweit verbreitende und Schaden stiftende Viren (z. B. Melissa, I-love-you) und spektakuläre Hacker-Einbrüche in sicherheitskritische Computer und Netze zeigen immer wieder die Verletzlichkeit der heutigen Informations- und Kommunikationstechnik. Gefährdungen entstehen im Internet-Zeitalter vor allem durch umfangreiche Vernetzung, Komfortoberflächen und Automatismen ohne durchschaubare Struktur sowie teilweise umgekehrt durch allgemeine Verfügbarkeit der Quellprogramme; zusätzliche Gefahren treten auf durch die zunehmende eMail- und Internet-Nutzung an jedem Arbeitsplatz. Dem versuchen technische und organisatorische Maßnahmen zu begegnen; Virenscanner, Firewall-Abschottung interner Netze und Adress-Translation zur Absicherung der internen Akteure sind weitgehend selbstverständlich. Letztendlich scheitern diese Absicherungen im Ein-

zelfall aber immer wieder an mangelhafter Implementation und Konfiguration durch fehlendes Know-How oder Nachlässigkeit bzw. Bequemlichkeit bei den verantwortlichen Systemadministratoren und Anwendern. Vorsätzliche externe Angriffe sind damit ebenso möglich wie Fehler, die von eigenen Mitarbeitern aus Spielerei, Neugier oder dem Versuch begangen werden, ihre eigene Überlegenheit zu beweisen.

Behandelt man jedoch den eigenen PC auch im geschlossenen internen Netz so, als wäre er ans Internet angeschlossen (gesundes Basis-Misstrauen, ausreichende Schutzvorkehrungen auch ohne Rücksicht auf schon getroffene Maßnahmen im Netz), hat man eigentlich schon das Wesentliche gegen solche Gefahren getan.

Vor allem auch als Hilfe für die Administratoren, die für die sichere Konfiguration von Hard- und Software verantwortlich sind, habe ich mit Blick auf einen solchen PC-Arbeitsplatz versucht, die damit verbundenen Risiken und geeignete Maßnahmen dagegen zu beschreiben. Diese Beschreibung ist in meinem Internet-Angebot abrufbar.

3 Übergreifende Themen

Die aktuelle Diskussion zu manchen Fragen lässt sich so schwer einzelnen Fachbereichen zuordnen, dass ich sie gesondert darstellen möchte.

3.1 Serviceorientierte Verwaltung

Nahezu alle öffentlichen Stellen bemühen sich, in einer „modernen Verwaltung“ ihre Dienstleistung für den Bürger leichter zugänglich zu machen, insbesondere hierbei den unmittelbaren Kontakt mit ihm zu erleichtern. Hierzu dienen gesonderte – möglichst gut erreichbare - Anlaufstellen, über die persönlicher Kontakt mit verschiedenen Ämtern aufgenommen werden kann. Immer größere Bedeutung erlangt aber auch die Telekommunikation, die sogar erlaubt, Bürger interaktiv an Verfahren mit automatisierter Datenverarbeitung teilnehmen zu lassen.

Vorreiter der Entwicklung, auf die ich im letzten Bericht bereits hingewiesen habe, waren die Kommunen mit “Bürgerbüros“, in denen eine rasche Information, eine schnellere Bearbeitung einfacher Verwaltungsvorgänge und eine umfassendere Bürgerberatung als mit einem einzelnen Fachamt angeboten werden soll. Im vergangenen Jahr hat die Finanzverwaltung mit den Servicestellen in den Finanzämtern vergleichbare Hilfen aufgenommen, und auch die obersten Landesbehörden wollen mit sogenannten Bürgerberatern im Kompetenzwirrwarr dem Bürger mit Rat und Tat zur Seite stehen.

In den Anfangszeiten dieser kundenfreundlichen Ausrichtung wurde der Gesichtspunkt des Datenschutzes nur allzu oft schlichtweg vergessen. Noch

immer gibt es Fälle, in denen die Möglichkeit eines Mithörens von Gesprächen oder gar Mitlesens auf Bildschirmen in Großraumbüros besteht. Hinweise auf die Möglichkeit vertraulicher Gespräche mit einem Bediensteten außerhalb dieses Büros sollten selbstverständlich sein; sie ersetzen aber nicht die kundenfreundliche Umgestaltung der Räume, wenn Datenschutzaspekte nicht schon bei der Planung beachtet wurden. In verschiedenen Fällen habe ich – manchmal erst nachträglich – mit Erfolg auf ihre Beachtung hinwirken können.

Schwieriger als dies sind Probleme beim Einsatz der elektronischen Datenverarbeitung in diesen Büros und der Kommunikation zwischen den verschiedenen Funktionseinheiten der öffentlichen Stellen, vor allem aber beim unmittelbaren Kontakt mit den Bürgern. Genaue Abstufung der Zugriffsrechte, Sicherungen gegen unberechtigte Eingriffe, zuverlässige Authentifizierung – das sind nur einzelne Fragen, die auf der Basis einer ordentlichen Risikobewertung mit einem schlüssigen Sicherheitskonzept beantwortet werden müssen.

Immer wieder stelle ich auch bei den Internet-Angeboten der öffentlichen Stellen fest, dass Homepages in erheblichem Umfang personenbezogene Daten enthalten. Häufig ist diesen Stellen nicht einmal bewusst, dass es sich hierbei um die Verarbeitung personenbezogener Daten handelt. Die Gefahren gerade des Internet mit der leichten und nicht kontrollierbaren automatisierten Weiterverarbeitung sind vielfach immer noch nicht bekannt oder werden in dem euphorischen Bemühen unterschätzt, bei dessen Nutzung an der Spitze des Fortschritts zu sein. Leider sind meine Hinweise im „Merkblatt über Anforderungen an Internet-Angebote und die Internet-Nutzung öffentlicher Stellen“, das ich im November 1999 den öffentlichen Stellen zugeleitet hatte, vielfach nicht beachtet worden.

Ich habe deswegen zusätzlich als Arbeitshilfe für die Verwaltungen Empfehlungen versandt, die unter Federführung meiner Kollegin in Nordrhein-Westfalen von einer Arbeitsgruppe der Datenschutzbeauftragten erstellt worden sind (vgl. Entschließung vom 12./13.10.2000, Anlage 21). Darin wird der Versuch unternommen, Fragen des Datenschutzes und der Datensicherheit zu verschiedenen Aspekten einer „modernen“ Verwaltungsausrichtung zusammenfassend darzustellen. Die Broschüre stellt in acht Kapiteln folgende Themen aus der Sicht des Datenschutzes dar:

- Multifunktionaler Service: Bürgeramt, Bürgerbüro, Bürgerladen und Kundencenter
- Call-Center
- Informationsangebote öffentlicher Stellen im Internet
- Interaktive Verwaltung

- Bürgerkarte
- Elektronische Auskunft, Akteneinsicht und Bürgerbeteiligung
- Auslagerung von Verwaltungsfunktionen.

Der Text der Broschüre ist unter www.lfd.niedersachsen.de zugreifbar.

3.2 Videoüberwachung

Haben wir uns schon daran gewöhnt, dass fast überall in Banken, Tankstellen und Kaufhäusern Kameras auf uns gerichtet sind? Dass unser Verhalten nicht nur von Touristen aufgezeichnet wird, für die wir Komparsen vor dem architektonisch interessanten Gebäude sind, sondern auch von Sicherheitsdiensten und von privaten Bildersammlern? Gibt es, wo wir uns anderen zeigen, Schranken gegen Techniken, die das heimliche und dauerhafte Festhalten des Bildes möglich machen?

Optisch-elektronische Beobachtung mit sprunghaft verbesserter und zugleich preiswerter gewordener Technik ermöglicht die Kontrolle von Produktionsprozessen, die Sicherung vor Gefahren und die Erinnerung an die schönsten Urlaubserlebnisse. In breitem Umfang wird sie zum Eigentumsschutz innerhalb privater Gebäude eingesetzt. Zunehmend findet sie Verbreitung in Bereichen, die faktisch einer größeren Öffentlichkeit zugänglich sind.

Pauschal kann man nicht bewerten, ob dies verdammenswert oder zu begrüßen ist. So empfinden Betroffene den Einsatz dieser Technik manchmal als sinnvoll, ja als notwendig, während er an anderer Stelle und unter anderen Umständen als problematisch oder gar als gänzlich unvertretbar angesehen werden muss. Diese Ambivalenz hängt neben dem Umfeld – vor allem dem Bestehen von Gefahren – wesentlich auch davon ab, wie transparent die Verarbeitung ist, ob also Aufnahmen überhaupt bemerkt werden und welche Art der Nutzung vorstellbar ist.

Weil für den Einzelnen oft nicht erkennbar ist, ob, von wem, in welcher Weise und wofür Aufnahmen gefertigt werden und ob sie über das flüchtige Betrachten hinaus dauerhaft gespeichert bleiben, kann dies sein Verhalten beeinflussen, sogar gravierend seine Entscheidungsfreiheit beeinträchtigen. Dies muss er – wie bei jeder anderen Datenverarbeitung auch, – nur hinnehmen, wenn er hierin eingewilligt hat oder eine Rechtsgrundlage dies erlaubt. Momentan ist aber die Rechtslage keineswegs eindeutig. Zwar gibt es gegen die Verbreitung von Aufnahmen eine Regelung im Kunsturheberrechtsgesetz; im übrigen ist aber gerade für die Aufnahmen als solche und ihre Verarbeitung nur wenig in Rechtsvorschriften bestimmt, wenn man von einzelnen Bestimmungen für die Tätigkeit der Sicherheitsorgane absieht.

Der Bedarf hierfür ist – besonders für Bereiche, in denen Personen in öffentlichem Raum einer Beobachtung mit optisch-elektronischen Mitteln ausgesetzt sind – aber groß, damit der sich entwickelnde Wildwuchs in geordnete Bahnen kommt und sich nicht beängstigende Zustände entwickeln, bei denen Menschen einer flächendeckenden Kontrolle durch unbekannte Mächte ausgesetzt sind. Seit Jahren fordern die Datenschutzbeauftragten, bei der Modernisierung des Datenschutzes auch eine Lösung dieses Problems anzugehen.

In einer gesonderten Entschließung vom 14./15.3.2000 (Anlage 13) haben sie auf die Risiken hingewiesen und klare Grenzen gefordert, die differenzierend für öffentliche Stellen und den privaten und geschäftlichen Bereich gesetzt werden müssen. Maßgeblich wird hierin gefordert, dass

- eine strenge Zweckbindung,
- eine differenzierte Abstufung zwischen Übersichtsaufnahmen, dem gezielten Beobachten einzelner Personen, dem Aufzeichnen von Bilddaten und dem Zuordnen dieser Daten zu bestimmten Personen,
- die deutliche Erkennbarkeit der Videoüberwachung für die betroffenen Personen,
- die Unterrichtung identifizierter Personen über die Verarbeitung ihrer Daten sowie
- die Löschung der Daten binnen kurzer Fristen

strikt sichergestellt werden.

Im Entwurf für ein neues Bundesdatenschutzgesetz ist inzwischen eine Vorschrift enthalten, die für den nichtöffentlichen Bereich, wo es bisher an Regelungen fehlt, in knapper Form eine Leitlinie setzt, aber die Forderungen längst nicht so differenziert aufnimmt wie gewünscht. Möglicherweise ergibt sich in der parlamentarischen Beratung noch eine weitere Differenzierung.

Für die öffentlichen Stellen im Saarland ist zwischenzeitlich mit der Novelle zum Saarländischen Polizeigesetz eine Entscheidung getroffen, die den Einsatz dieser Technik durch die Vollzugspolizei an öffentlich zugänglichen Orten regelt (vgl. TZ 6.1). Auch sie ist nicht so differenziert, wie ich es erhofft habe. Mit der ausdrücklichen Regelung ist aber andererseits zugleich klargestellt, dass anderen Behörden diese Befugnis nicht zusteht.

3.3 “Data Warehouse” und „Data Mining“

Nicht nur im geschäftlichen Bereich gibt es den Wunsch, die häufig an verschiedenen Stellen und zu unterschiedlichen Zwecken gespeicherten Daten zentral verfügbar zu machen und Erkenntnisse zu gewinnen, die erst die Zusammenschau möglich macht. Unter Einsatz statistischer Methoden lassen sich – auch ohne hypothetische Fragestellungen, die durch das Daten-

material bestätigt oder verworfen werden – aus der Verknüpfung ggf. völlig ungeahnte Zusammenhänge erschließen, die zu weiteren Zwecken genutzt werden.

Wenn hiervon personenbezogene Daten betroffen sind, bricht dies offensichtlich mit dem zentralen datenschutzrechtlichen Grundsatz der Zweckbindung, also dem Gebot, die für einen definierten Zweck erhobenen Daten nur in diesem Zusammenhang zu nutzen und nicht ohne Einwilligung oder gesetzliche Grundlage anderweitig zu verwenden. Zugleich entspricht dies meist ebenfalls nicht dem Transparenzgebot, weil der Betroffene die Art und Zielrichtung gar nicht mehr erkennen kann. Die Gefahr, dass unzulässige Persönlichkeitsprofile entstehen und Entscheidungen allein automatisiert getroffen werden, liegt nahe. Oftmals ist es aber auch gar nicht das Ziel, auf einzelne bestimmbare Personen bezogene Erkenntnisse zu gewinnen; dann genügt die Verwendung anonymisierter oder pseudonymisierter Daten, die dann datenschutzrechtlich unproblematisch ist, wenn jegliche Reidentifikation ausgeschlossen ist.

Noch bezieht sich die Mehrzahl der in Betracht gezogenen Anwendungen auf den nicht-öffentlichen Bereich, für den meine Zuständigkeit nicht gegeben ist. Allerdings gibt es Überlegungen, die Methoden und Verfahren etwa auch in der Personalverwaltung und selbstverständlich bei erwerbswirtschaftlich tätigen Stellen einzusetzen. Und die Erfahrung zeigt, dass einmal verfügbare Werkzeuge, wenn sie erfolgreich im privaten Bereich genutzt werden, auch von den öffentlichen Stellen verwendet werden. Deshalb halten es die Datenschutzbeauftragten des Bundes und der Länder, auch soweit ihnen nicht die Kontrollkompetenz im Wirtschaftssektor obliegt, für notwendig, sich frühzeitig mit der Problematik zu befassen.

Mit ihrer Entschließung vom 14./15.3.2000 (Anlage 15) haben sie einzelne Aspekte aufgezeigt sowie Hersteller und Anwender aufgerufen, mit der Verwendung datensparsamer Technologien Datenschutzgefahren zu vermeiden.

3.4 Systemdatenschutz, freie Telekommunikation

Die Forderung nach Datenvermeidung und Datensparsamkeit und nach Systemdatenschutz als technische Vorkehrung gegen Gefährdungen der Privatheit, denen normative Ge- und Verbote nicht ausreichend begegnen können, ist ebenfalls wesentlicher Inhalt weiterer Entschließungen. Wichtig werden diese Gesichtspunkte vor allem in der Telekommunikation, die zunehmende Bedeutung für unseren Alltag hat. Die hier vielfach entstehenden Spuren sollten reduziert und nicht für mögliche andere Zwecke bewusst erweitert und konserviert werden.

Weil damals marktführende Firmen Bauteile und Verfahren verbreiteten, die – für Nutzer gar nicht oder wenig durchschaubar – deren personenidentifizierbare Daten erheben und verwenden konnten, haben die Datenschutzbeauftragten von Bund und Ländern sich im Frühjahr 1999 gegen solche Praktiken ausgesprochen. An die entsprechenden Hersteller wurde appelliert, Hard- und Software so zu entwickeln und herzustellen, dass Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit von Sicherheitsvorkehrungen überzeugen können, und den Anwendern empfohlen, nur solche Produkte einzusetzen, welche auch eine Transparenz der Verfahrensabläufe gewährleistet. (Anlage 3).

Andererseits sollten die Verfahren und Produkte geeignet sein, die vom Nutzer vorausgesetzte Vertraulichkeit bei der Kommunikation auch zu garantieren. Hierfür kommen vor allem Verschlüsselungsverfahren in Betracht, die leicht handhabbar sein sollten und keine unangemessenen „Hintertüren“ aufweisen. Bei der Verarbeitung sensibler Daten sind derartige Verfahren auch im öffentlichen Bereich – vor allem für die Kommunikation zwischen externen Stellen – unabdingbar. Im Hinblick auf die jahrelange politische Kontroverse über die deutsche Kryptopolitik haben die Datenschutzbeauftragten 1999 die Öffnung zu einer generell freien Verfügbarkeit von Verschlüsselungsprodukten ausdrücklich begrüßt und die öffentlichen Stellen aufgefordert, beispielhaft daran mitzuwirken, dass Kryptographie Standard in der Informations- und Kommunikationstechnik wird (Anlage 11).

Mit besonderer Sorge war im Telekommunikationsbereich die Entwicklung zu immer aussagekräftigeren Daten zu beobachten, die – sogar ohne die eigentlichen Inhalte – als Verbindungs- Nutzungs- und Abrechnungsdaten eine detaillierte Auswertung und Verknüpfung mit anderen Informationen erlauben. Mit Abwicklung von verschiedensten Geschäften im Internet fallen weitere Spuren an, die ebenfalls das Interesse privater wie öffentlicher Stellen wecken. Tatsächlich ist ein deutlich zunehmender Zugriff der Sicherheitsorgane auf diese Daten zu verzeichnen, und in verschiedenen Zusammenhängen zielen Gesetzgebungsvorhaben auf eine Absicherung und Erweiterung dieser Möglichkeiten. Ein zusammenfassendes, in sich schlüssiges System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf unbeobachtete Kommunikation unter Berücksichtigung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt, fehlt aber bisher.

Mit Forderungen zur Gewährleistung der freien Telekommunikation haben die Datenschutzbeauftragten sich im März 2000 an Gesetzgebung und Verwaltung gewandt (Anlage 14). Die Entschließung zeigt die Problematik auf und wendet sich gegen die Vernachlässigung des Telekommunikationsgrundrechts gegenüber Sicherheitsbelangen, richtet sich keineswegs einsei-

tig gegen diese, sondern verlangt wirksamen Schutz der Privatsphäre gerade auch gegen illegale Aktivitäten im nichtöffentlichen Bereich.

4 Allgemeines Datenschutzrecht

4.1 Europäischer Datenschutz

4.1.1 Datenschutz als Grundrecht

Seit langem fordern nicht nur die Datenschutzbeauftragten (in Deutschland und anderen Staaten der EU), auch auf der Ebene des Europäischen Primärrechts den Datenschutz als Grundrecht zu verankern; hierauf hatte ich bereits im 16. TB hingewiesen (TZ 6.1 mit Anlage 5). Meine Kollegen und ich haben in einer erneuten Entschließung vom 7./8.10.1999 (Anlage 9) den damaligen Beschluss des Europäischen Rates nachhaltig unterstützt und die Gesetzgebungsorgane des Bundes aufgefordert, sich für eine schriftliche Verankerung des Grundrechts in den Verträgen der EU einzusetzen.

Mit der feierlichen Proklamation der Europäischen Grundrechtscharta in der Regierungskonferenz in Nizza im Dezember 2000 sind diese Bemühungen einen großen Schritt vorangekommen. Zwar ist die Charta bislang kein formelles Recht; die breite Zustimmung auch im Europäischen Parlament lässt aber hoffen, dass der Grundrechtskatalog mittelfristig in die Europäischen Verträge aufgenommen und damit rechtsverbindlich wird. Dies ist unerlässlich, damit in einer Welt mit zunehmenden internationalen Kontakten und Kommunikationsströmen und mit immer bedeutsamerer Rechtsetzung durch die Europäische Union ausreichender Schutz gewährleistet ist, auf den man sich gegenüber den Europäischen Organen, zugleich aber auch nationalen Stellen des eigenen Landes oder anderer Mitgliedsstaaten berufen kann, wenn diese Unionsrecht ausführen. Über die Beachtung bei den EU-Stellen muss eine eigene unabhängige Kontrollinstanz wachen.

Wie effektiv der tatsächliche Schutz durch das Grundrecht ist, bestimmt sich aber nicht allein aus dessen Formulierung, sondern wesentlich danach, wie intensiv die - selbstverständlich nötigen - Schranken das Recht inhaltlich bestimmen. Während die Grundrechtscharta in der Mehrzahl der Rechte auf konkrete Begrenzungen verzichtet und vielmehr alle Grundrechte unter eine eher allgemein gehaltene Generalklausel-Schranke stellt, sind für den Datenschutz immerhin zentrale Grundsätze festgelegt: Datenverarbeitung „nach Treu und Glauben“ und nur aufgrund Einwilligung oder gesetzlicher Grundlage; Zweckbindung; Auskunftsrecht; unabhängige Kontrollinstanz. Jedenfalls muss (letztlich durch die Rechtsprechung des Europäischen Gerichtshofs) ausgeschlossen sein, dass der gewollte Freiheitsschutz unter Hinweis auf „von der Union verfolgte Zielsetzungen von allgemeinem Inter-

esse“ oder „andere legitime Interessen in einer demokratischen Gesellschaft“ faktisch ausgehöhlt wird.

4.1.2 Datenverkehr mit „Drittländern“

Die Harmonisierung des Datenschutzes auf europäischer Ebene soll vor allem einen leichteren, von bürokratischen Hemmnissen freien Transfer auch personenbezogener Daten im Handel und Dienstleistungsverkehr erreichen. Dementsprechend wird im Binnenmarkt prinzipiell nicht mehr zwischen Inland und den übrigen Mitgliedsstaaten unterschieden, bei denen ja - wegen der Harmonisierung - ein gleichwertiger Datenschutzstandard gewährleistet ist, wenn auch die Anforderungen im Einzelnen differieren mögen.

Damit für den ebenfalls häufigen Verkehr mit Stellen in Staaten außerhalb der Europäischen Union nicht jeweils auf das Einverständnis der Betroffenen zurückgegriffen werden muss, lässt Art. 25 der EG-Richtlinie grenzüberschreitende Datenübermittlungen auch dann zu, wenn die Europäische Kommission feststellt, dass im jeweiligen Drittland ein „angemessenes Schutzniveau“ gewährleistet ist. Für eine Reihe von (überwiegend europäischen) Staaten ist dies inzwischen erfolgt. Diese Entscheidung ist insbesondere dann schwierig zu treffen, wenn deutliche Strukturunterschiede im Rechtssystem bestehen. Im – für den Datentransfer bedeutsamen - Verhältnis zu den USA wird ein angemessenes Schutzniveau für solche Stellen angenommen, die sich den mit der Kommission abgesprochenen Grundsätzen des „sicheren Hafens“ unterworfen haben, zu denen auch die Möglichkeit einer Kontrolle gehört.

4.2 Bundesdatenschutzgesetz

Trotz der durch die EG-Datenschutzrichtlinie gesetzten Anpassungsfrist, die bereits im Oktober 1998 abgelaufen war, konnte die Novellierung des wichtigsten Datenschutzgesetzes des Bundes noch nicht abgeschlossen werden. Immerhin gab es die parlamentarische Behandlung eines Entwurfs, der - im wesentlichen auf der Basis von Vorarbeiten noch aus der früheren Wahlperiode, aber teilweise ergänzt – in einer „ersten Stufe“ die dringlichsten Punkte in Angriff genommen hat. Für eine zweite Stufe – möglichst noch in dieser Wahlperiode – sind weitere Schritte auf dem Weg in Aussicht genommen, das Datenschutzrecht zu modernisieren. Die Koalitionsfraktionen und die Bundesregierung bereiten dies mit Gutachten und unter Beteiligung von Sachverständigen vor, bei der auch die Datenschutzbeauftragten zu Wort kommen werden.

Selbstverständlich ist dieses Thema ständiger Punkt in den Zusammenkünften der Datenschutzbeauftragten des Bundes und der Länder. Im jeweiligen Verfahrensschritt haben meine Kollegen und ich mit den Entschließun-

gen vom 25./26.03.1999 und 12./13.10.2000 (Anlagen 1 und 22) an Bundesregierung, Bundestag und Bundesrat auf die Dringlichkeit und auf notwendig erscheinende Einzelaspekte hierbei hingewiesen.

4.3 Saarländisches Datenschutzgesetz

Wie das BDSG hätte, wie bereits in den vorangegangenen beiden Berichten dargestellt, innerhalb der dreijährigen Frist seit Erlass der EG-Datenschutzrichtlinie auch das SDSG an deren Vorgaben angepasst sein müssen. Hierauf wurde aber mit Blick auf die noch nicht abgeschlossene Rechtsetzung auf Bundesebene bewusst abgesehen. So gab es – anders als in mehreren Ländern, in denen die Novellierung der allgemeinen Datenschutzgesetze teils abgeschlossen, jedenfalls aber eingeleitet wurde – im Berichtszeitraum seitens der Landesregierung hierzu keine nach außen erkennbaren Schritte.

Im Zusammenhang mit anderen Gesetzgebungsvorhaben, der Erörterung des letzten Tätigkeitsberichts und im Gespräch mit dem zuständigen Referat des Innenministeriums habe ich meinerseits bereits verschiedene Anregungen gegeben und werde selbstverständlich eingehend zu dem Entwurf der Landesregierung Stellung nehmen, wenn er mir zugänglich gemacht wird. Zu entscheiden wird auch sein, ob das Land an der unterschiedlichen Kontrollzuständigkeit für öffentlichen und nichtöffentlichen Bereich festhält.

Nachdem die EU-Kommission schon seit längerem beschlossen hat, Klage gegen die „säumigen“ Mitgliedsstaaten wegen der fehlenden Umsetzung zu erheben und der Bundesrepublik seit Ende 2000 die formelle Klageschrift vorliegt, dürfte der Druck mit finanziellen Sanktionen zur Beschleunigung des Gesetzgebungsverfahrens im Bund wie auch bei den Ländern führen, bei denen die Novellierung noch aussteht.

5 Justiz

Gerade im Justizbereich haben wir uns im Berichtszeitraum mit einer Vielzahl von Vorhaben befassen müssen, die länderübergreifenden Charakter haben oder die Änderung bundesrechtlicher Normen oder deren Umsetzung betreffen. In einer Reihe von Fällen hat die Konferenz der Datenschutzbeauftragten – teils aus aktuellem Anlass – mit Entschließungen gemeinsam Stellung bezogen, mehrfach sogar zu Änderungen im Strafprozess.

5.1 Strafverfahrensänderungsgesetz 1999

Die Forderung der Datenschutzbeauftragten nach bereichsspezifischen datenschutzrechtlichen Regelungen im Strafverfahren reicht bis in die Anfangszeiten der Datenschutzkontrollinstanzen zurück; mehrfach habe ich hierüber berichtet.

Im Jahre 2000 wurde endlich das Strafverfahrensänderungsgesetz 1999 in Kraft gesetzt. Es entspricht den Vorstellungen der Datenschutzbeauftragten letztlich aber nur teilweise, auch wegen zahlreicher Kompromisse, die im Gesetzgebungsverfahren insbesondere auf Drängen des Bundesrates geschlossenen wurden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sah sich daher veranlasst, noch im Frühjahr des Jahres 2000 zum damaligen Entwurf in einer Entschließung darauf hinzuweisen, dass zwar das Schaffen von Normen in der Strafprozessordnung, die ein angemessenes Datenschutzniveau gewährleisten sollen, grundsätzlich zu begrüßen ist, dass aber die Lösungen aus der Sicht des Datenschutzes unbefriedigend bleiben (Anlage 17).

Nach Inkrafttreten des Gesetzes zeichnen sich schon jetzt Auslegungsschwierigkeiten bei einzelnen Fallgestaltungen ab, die möglicherweise eine Nachbesserung des Gesetzgebers erfordern. Zunächst ist aber der Rechtsprechung eine Chance einzuräumen, bei der Umsetzung des Strafverfahrensänderungsgesetzes 1999 einen verbesserten Persönlichkeitsschutz zu erreichen.

5.2 Aufbewahrung des Schriftgutes der Justiz

Zu den noch fehlenden bereichsspezifischen Regelungen im Justizbereich zählen die Aufbewahrungsbestimmungen für das Schriftgut der Justiz. Bislang sind Vorgaben hierzu nur in der Form von Verwaltungsvorschriften vorhanden. Die Diskussion über die Frage, ob es insofern einer gesetzlichen Regelung bedarf, hat bereits eine mehrjährige Geschichte.

In neuerer Zeit beginnt sie mit einer Entschließung der Datenschutzbeauftragen des Bundes und der Länder aus dem Jahre 1995 (TZ 12.6 und Anlage 12 des 16. TB) und hat sich in einer Entschließung aus dem Jahre 1999 (Anlage 6) zum Schriftgut der ordentlichen Gerichtsbarkeit und der Staatsanwaltschaften fortgesetzt. Aus datenschutzrechtlicher Sicht kann es nicht zweifelhaft sein, dass der Gesetzgeber die grundlegenden Voraussetzungen für die Aufbewahrung selbst festlegen muss, da es sich hier um eine zweckändernde Datenverarbeitung handelt, wenn die Daten nach Abschluss eines Verfahrens zu außerhalb des eigentlichen Verfahrens liegenden Zwecken weiterhin aufbewahrt werden. In der letzten Entschließung wurde daher auch auf gerichtliche Entscheidungen hingewiesen, die diese Rechtsauffassung bestätigen; als gesetzgeberische Aufgabe dürfe die Normierung nicht nur mittelfristig geplant werden, sondern sei alsbald in Angriff zu nehmen.

Erfreulicherweise ist das Saarland ebenso wie einige andere Bundesländer für eine gesetzliche Regelung in der von der Justizministerkonferenz gebildeten Arbeitsgruppe „Aufbewahrungsbestimmungen“ eingetreten.

Es ist davon auszugehen, dass die Datenschutzbeauftragten des Bundes und der Länder das Novellierungsvorhaben mit konstruktiven Vorschlägen begleiten werden.

5.3 Umsetzung des DNA-Identitätsfeststellungsgesetzes

Mit dem DNA-Identitätsfeststellungsgesetz wurde die Möglichkeit geschaffen, in eine zentrale Genomanalysedatei (DNA-Datei) beim Bundeskriminalamt identifizierende Informationen von Personen einzuspeichern, die in künftigen Strafverfahren möglicherweise als Täter in Betracht kommen. Diese rein vorsorgliche Speicherung zur Erleichterung der Beweisführung ist selbstverständlich nur im Hinblick auf schwere Straftaten und bei hinreichenden Momenten für eine mögliche Täterschaft zu rechtfertigen; deshalb bindet das Gesetz die Entscheidung an hohe materielle und verfahrensmäßige Voraussetzungen. Während im Zusammenhang mit einer einzelnen aktuellen Verurteilung Informationen auch für derartige Entscheidungen verfügbar sind, wurde bei Umsetzung des Gesetzes offenkundig, wie aufwändig nachträgliche Überprüfungen anhand von Altfällen über frühere Straftäter werden, deren Daten der Gesetzgeber ebenfalls in die Zentraldatei integrieren wollte. Allein im Saarland waren nach Darlegung der Staatsanwaltschaft fast 11.000 Personaldatensätze mit dem Ziel zu überprüfen, ob es auch zum gegenwärtigen Zeitpunkt noch gerechtfertigt ist, bei einem früheren Straftäter eine Genomanalyse vorzunehmen.

Positiv hervorzuheben ist im Saarland die restriktive Überprüfungspraxis der Staatsanwaltschaft. Mittels der Kriterien „Straffreiführung“, „Alter“, „Gewicht des Deliktes“ hat sie eine Abschichtung der 11.000 Altfälle streng orientiert am Verhältnismäßigkeitsgrundsatz vorgenommen, so dass nach eigener Darstellung nur noch ein Viertel bis ein Drittel der überprüften Straftäter letztlich einer DNA-Analyse zu unterziehen waren. Es handelte sich damit immerhin noch um eine Anzahl von mehreren Tausenden von Straftätern, für die das Einholen einer richterlichen Anordnung für die Durchführung der Analyse und die Aufnahme in die DNA-Datei in Betracht kam. Dass die Staatsanwaltschaft dennoch nicht die Tendenz zeigte, sich den Aufwand zu erleichtern, war beachtenswert.

Ich habe es sehr begrüßt, dass hier insoweit von vornherein Einvernehmen in der Frage bestand, dass als rechtfertigende Grundlage nicht eine - bei im Strafvollzug Einsitzenden hinsichtlich ihrer Freiwilligkeit ohnehin problematische - Einwilligung des (ehemaligen) Straftäters zur DNA-Analyse in Betracht kommt. Dieser kann nur schwerlich für sich selbst die belastende Prognose stellen, er sei zukünftig in die Reihe der Wiederholungstäter einzu-

ordnen. Da dies in anderen Bundesländern unterschiedlich gehandhabt wurde, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder diese Praxis in einer Entschließung als unzulässig erachtet (Anlage 8). Die Maßnahme ist nach ihrer Auffassung nur aufgrund einer richterlichen Anordnung zulässig, nicht jedoch auf der Grundlage einer Einwilligung. Die Bedeutung des Richtervorbehalts für die Anordnung der Analyse hat inzwischen das Bundesverfassungsgericht ausdrücklich herausgehoben und dabei betont, dass es hierbei um eine echte Einzelfallprüfung ohne bloß formelhafte Bezugnahme auf die gesetzlichen Voraussetzungen gehen müsse.

5.4 Täter-Opfer-Ausgleich und Datenschutz

Auch die gesetzliche Regelung des Täter-Opfer-Ausgleichs, die die Strafprozessordnung jetzt getroffen hat, ist für den Datenschutz kein voller Erfolg geworden. Eher hat sich hier die des öfteren geäußerte Befürchtung bewahrheitet, der Gesetzgeber werde mit neuen Normen den in der Praxis bestehenden Datenschutz nicht verbessern, sondern verschlechtern.

Die Rechtsmaterie war zuvor in einer Landes-Richtlinie des Ministeriums der Justiz zur Förderung des Täter-Opfer-Ausgleichs bei Erwachsenen vom 18.6.1996 geregelt. Nach der dort festgelegten Definition soll es sich bei dem Täter-Opfer-Ausgleich um Bemühungen handeln, die nach einer Straftat zwischen Täter und Geschädigtem bestehenden Probleme, Belastungen und Konflikte zu bereinigen. Er soll insbesondere auch die Möglichkeit bieten, die bisher im Strafverfahren oft vernachlässigten Opferbelange zu berücksichtigen. Betont wurde in der Richtlinie, der Schlichter, bei dem es sich im Saarland ausschließlich um den Sozialdienst der Justiz handelt, solle nicht versuchen, das Opfer zu dem Verfahren zu überreden.

Weil sich im Gesetzgebungsverfahren jedoch eine solche Tendenz abgezeichnet hatte, haben die Datenschutzbeauftragten mit ihrer Entschließung zu dieser Thematik dem zu begegnen versucht (Anlage 12).

Leider hat der Gesetzgeber den Opferinteressen nicht gleichgewichtig mit den Interessen des Straftäters Rechnung getragen: im Gesetz ist nunmehr festgehalten, dass nur noch der ausdrücklich geäußerte entgegenstehende Wille des Verletzten den von staatlichen Stellen vorgeschlagenen Täter-Opfer-Ausgleich verhindern kann. In einem Literaturbeitrag wurde sogar hervorgehoben, der Täter-Opfer-Ausgleich habe sich in der Praxis zu einem ausgesprochenen „Strafrabatt“ für den Täter entwickelt und sei daher von dieser Seite durchweg zu begrüßen.

Wie ich Presseberichten entnehmen konnte, soll eine neue Richtlinie des Justiz- und Innenministeriums ergehen, wonach bereits die Polizei abklären soll, ob eine Konfliktbereinigung angestrebt wird. Den Opfern könnte dies einige für sie unzumutbare Konfrontationen ersparen.

5.5 Parlamentarische Kontrolle von Lauschangriffen

Das Abhören des nicht-öffentlich gesprochenen Wortes in Wohnungen durch staatliche Stellen ist ein gravierender Eingriff in das Grundrecht nach Art. 13 GG, das den Schutz der Privatheit in diesem engsten Lebensbereich schützt. Mit der Einführung des “Großen Lauschangriffs“ zu repressiven Zwecken hat der Gesetzgeber in Art. 13 Abs. 6 GG eine besondere parlamentarische Kontrolle vorgeschrieben. Sie dient – unter Berücksichtigung der besonderen Sensibilität der Maßnahme - der in der Demokratie stets gebotenen Kontrolle exekutiver Tätigkeit, zugleich aber wesentlich auch der Bewertung des Gesetzgebers selbst, ob und inwieweit überhaupt derartige Eingriffe geeignete und angemessene Mittel staatlichen Handelns sind und bleiben müssen. Dazu korrespondierend sind auch in der Strafprozessordnung Berichtspflichten der Staatsanwaltschaft gegenüber der zuständigen obersten Justizbehörde und der Bundesregierung gegenüber dem Bundestag auf der Grundlage von Ländermitteilungen eingeführt worden.

Schon der erste Bericht ließ allerdings die Besorgnis aufkommen, dass die Aussagekraft nicht ausreicht, wenn nur die Gesamtzahl der von der Anordnung Betroffenen – lediglich unterschieden zwischen beschuldigten und nicht beschuldigten Wohnungsinhabern - wiedergegeben wird. Es fehlten insbesondere Angaben über die Zahl der tatsächlich abgehörten Personen, die Art der abgehörten Räume (Geschäftsräume, Wohnungen, Restaurants usw.), die Anzahl und Dauer der angeordneten Verlängerungen der Maßnahme, die Zahl der Verhaftungen, Anklagerhebungen und Verurteilungen, zu denen die Maßnahme beigetragen hat.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher in einer Entschließung (Anlage 20) solche zusätzlichen Kriterien aufgeführt, nach denen die Einzelfälle des „Großen Lauschangriffs“ einer effektiven parlamentarischen Kontrolle unterzogen werden können. Effektiv heißt in der Praxis unserer Demokratie allerdings auch, dass die Diskussion – natürlich nicht der personenbeziehbaren Einzelumstände, sondern der im Bericht zu nennenden Gesamtdaten – im Plenum stattfindet und nicht in ein geheim tagendes Gremium verbannt wird.

Dass die parlamentarische Kontrolle auch in den Ländern, die das Grundgesetz ebenfalls anordnet, in gleicher Weise wie im Bund effektiv sein muss, habe ich gegenüber dem Landtag und dem Justizministerium mit Übersendung der genannten Entschließung geltend gemacht. Auch insoweit muss den zuständigen staatlichen Organen eine ausreichende Einflussmöglichkeit auf den umsichtigen Gebrauch dieser schwerwiegenden Maßnahme eingeräumt werden. Zwischenzeitlich liegt dem Landesparlament der jährliche Bericht der Landesregierung zu den präventiven und repressiven Maßnahmen zur Wohnraumüberwachung vor.

5.6 Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation

Ende 2001 wird die gesetzliche Befristung des § 12 Fernmeldeanlagengesetz (FAG) auslaufen; das nahe Ende dieser vereinzelt übrig gebliebenen Bestimmung eines alten Gesetzes war schon wiederholt hinausgeschoben worden. Auch im Jahr 2001 wird der Gesetzgeber sich deshalb wiederum mit dem Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation befassen wollen, der in der Praxis große – sogar zunehmende – Bedeutung für die Ermittlungserfolge der Sicherheitsbehörden, umgekehrt aber auch für die Einbuße wesentlicher Freiheitsrechte der (oft gänzlich unschuldigen) Bürger hat, die von diesen Maßnahmen betroffen werden.

In einer Entschließung (Anlage 7) haben die Datenschutzbeauftragten des Bundes und der Länder betont, es handle sich bei dieser Bestimmung um eine Norm, die der heutigen Zeit nicht mehr entspricht. Sie erlaubt bei allen strafgerichtlichen Untersuchungen dem Richter und bei Gefahr im Verzug auch der Staatsanwaltschaft, Auskünfte über die Telekommunikation einzuholen. Die staatliche Überwachung in der Telekommunikation greift heute tief in das grundgesetzlich geschützte Telekommunikationsgeheimnis ein, weil die digitale Technik mit geringem Aufwand schnelle Auswertungen erlaubt. Den Verbindungsdaten kommt häufig die gleiche Aussagekraft zu wie den Inhaltsdaten. Aufgrund von Regelmäßigkeit und Häufigkeit von Verbindungen können zudem Persönlichkeitsprofile erstellt werden.

§ 12 FAG hat zwar gleichzeitig mit der letzten Befristung auf das Ende des Jahres 2001 eine Verbesserung dahingehend erfahren, dass die Daten unverzüglich unter Aufsicht der Staatsanwaltschaft zu vernichten sind, sobald sie zur Strafverfolgung nicht mehr benötigt werden. Die Betroffenen sind nunmehr auch grundsätzlich über die Maßnahmen zu benachrichtigen.

Dem zusätzlichen Verlangen der Datenschutzbeauftragten, den Zugriff auf Verbindungsdaten auf nicht unerhebliche Straftaten zu beschränken, wurde bislang jedoch nicht entsprochen. Bei der Vergleichbarkeit der Aussagekraft der Verbindungsdaten mit den Inhaltsdaten wäre dies hingegen nach Auffassung der Datenschutzbeauftragten in Anlehnung an die inhaltliche Überwachung der Telekommunikation geboten. Im erneuten Gesetzgebungsverfahren könnte dieser Forderung entsprochen werden.

5.7 Forschungsvorhaben im Justizbereich

Auch für die Strafverfolgung und –vollstreckung lassen sich gesicherte Erkenntnisse für Bewertung und Fortentwicklung gesetzlicher Regelungen oft nur gewinnen, wenn hierzu konkrete Einzelfälle herangezogen werden. Damit müssen aber Informationen über Einzelpersonen außerhalb der eigentli-

chen Verfahrenszwecke verarbeitet werden, und dies meist von Forschern, die der entsprechenden Justizverwaltung nicht angehören.

Für solche Untersuchungen, bei denen die Einwilligung der Betroffenen teilweise gar nicht in Betracht kommt, fehlten früher ausreichende Rechtsgrundlagen. Das Strafverfahrensänderungsgesetz 1999 hat sowohl eine neue allgemeine Rechtsgrundlage für Forschungsvorhaben im Strafverfahren geschaffen als auch eine spezielle Norm, nach der Forschungsvorhaben zu besonders evaluierungsbedürftigen Maßnahmen im Strafverfahren zulässig sein sollen.

Wissenschaftlicher Begleitung bedürfen vor allem solche Maßnahmen, die während des Verfahrens ohne Wissen der Betroffenen durchgeführt werden. Auskünfte aus Akten und Akteneinsicht können daher nunmehr ausdrücklich zu Forschungszwecken gewährt werden, durch die Aussagen zur Erforderlichkeit und Effizienz der sogenannten Rasterfahndung, der Telefonüberwachung, des sogenannten Lauschangriffs, des Einsatzes Verdeckter Ermittler und der längerfristigen Observation getroffen werden können. Seit der Einführung dieser verdeckten Maßnahmen haben nicht zuletzt die Datenschutzbeauftragten selbst die ständige Überprüfung dieser tiefen Eingriffe in die Persönlichkeitsrechte gefordert, von denen ja in der Anzahl überwiegend Dritte berührt werden, die mit dem strafrechtlichen Vorwurf nicht in Zusammenhang stehen.

Schon vor dem Inkrafttreten des Gesetzes hatte die Bundesregierung ein umfangreiches Forschungsvorhaben zu Telefonüberwachungen in Auftrag gegeben. Dessen Ergebnisse werden mit großem Interesse auch schon deshalb erwartet, weil der signifikante Anstieg der Telefonüberwachungen in der Bundesrepublik Deutschland bislang nicht befriedigend zu erklären ist.

Im Berichtszeitraum hatten wir auch ein Forschungsvorhaben im Maßregelvollzug zu bewerten. Dabei geht es um Daten von Straftätern, die wegen ihrer Unzurechnungsfähigkeit und Gefährlichkeit im Anschluss an ein Strafverfahren in einer geschlossenen Abteilung eines psychiatrischen Krankenhauses untergebracht sind. Informationen in diesen Zusammenhängen sind von großer Sensibilität; so finden sich in den dazugehörigen Akten regelmäßig auch Daten über die Herkunftsfamilie des Täters und ihre Struktur. Entsprechend kritisch muss auch die Forschung hiermit umgehen und mit anonymisierten Daten arbeiten, wo immer dies möglich ist.

Im konkreten Vorhaben habe ich rechtliche Einwände gegenüber dem ursprünglichen Konzept erhoben und Abhilfemöglichkeiten vorgeschlagen. Ich hoffe, dass meine Bedenken durch die Unterstützung der Staatsanwaltschaft und der Maßregelvollzugseinrichtung bei der Anonymisierung der Daten ausgeräumt werden konnten.

5.8 Bekanntgabe personenbezogener Daten durch Gerichte

Gerichtliche Prozesse werden in Deutschland normalerweise zwar öffentlich (mit der Möglichkeit des Zugangs zu den Verhandlungen und mittelbarer Berichterstattung hierüber) geführt, nicht aber in der Medienöffentlichkeit, die über unmittelbare Ton- und Bildübertragung an die Allgemeinheit auch außerhalb des Gerichtssaals jedem die Möglichkeit gibt, das Geschehen zu verfolgen. Lediglich für das Bundesverfassungsgericht waren bislang Ton- und Fernseh-Rundfunkaufnahmen in bestimmten Verfahrensabschnitten zulässig; eine entsprechende Vorschrift wurde auf Vorschlag der Landesregierung kürzlich auch für den Saarländischen Verfassungsgerichtshof beschlossen.

Das Bundesverfassungsgericht hat die derzeitige Rechtslage mit dem eingängigen Ausspruch "Prozesse finden in der Öffentlichkeit, aber nicht für die Öffentlichkeit statt" beschrieben und grundsätzlich bestätigt. Nach der jüngsten Entscheidung des Bundesverfassungsgerichts hat der Gesetzgeber es aber in der Hand zu bestimmen, inwieweit Prozesshandlungen für Fernsehkameras geöffnet werden sollen. Hierbei ist abzuwägen zwischen dem wichtigen Prinzip der Gerichtsöffentlichkeit, das ja Willkürjustiz ausschließen soll, und den Belangen der Betroffenen auf Achtung ihrer Privatheit.

Selbst bei der gegenwärtigen Rechtslage erreichen meine Dienststelle jedoch Beschwerden darüber, dass in Verhandlungen Umstände bekannt werden, die die Petenten gern vertraulich behandelt haben möchten, insbesondere wenn Krankheiten oder andere ähnliche Umstände aus dem persönlichen Lebensbereich erörtert werden müssen. Dem kann meist dadurch Rechnung getragen werden, dass der jeweilige Prozessvertreter (in der Regel ein Rechtsanwalt) den Ausschluss der Öffentlichkeit nach § 171b Gerichtsverfassungsgesetz beantragt, sofern nicht das Gericht selbst von seiner rechtlichen Befugnis, den Ausschluss der Öffentlichkeit anzuordnen, Gebrauch macht. Für andere Verfahrenshandlungen machen die jeweiligen Prozessordnungen ebenfalls Vorgaben zur Wahrung des Datenschutzes.

Auch wenn mich die Schilderung von Petenten, die in gerichtlichen Verfahrenshandlungen einen Datenschutzverstoß sehen, manchmal betroffen macht und auch ich keine rechtfertigende Erklärung hierfür finde, kann ich solchen Petenten konkrete Hilfen nicht geben. Zwar müssen datenschutzrechtliche Grundsätze selbstverständlich ebenfalls von der Rechtsprechung beachtet werden; mir ist aber eine Kontrolle wegen der zu achtenden Unabhängigkeit der Richter gesetzlich verwehrt. Ich empfehle jedoch hin und wieder, dass der Petent in seinem Prozess das Gespräch mit dem Richter auch über Datenschutzfragen anregt. Im übrigen verbleibt ihm, rechtskundige Hilfe (insbesondere bei Anwälten) nachzusuchen und fehlerhafte gerichtliche Handlungen mit Rechtsmitteln überprüfen zu lassen.

Die oben erwähnte Änderung des Gesetzes über den Saarländischen Verfassungsgerichtshof regelt im übrigen auch datenschutzrechtliche Einzelfragen neu, etwa zum Auskunfts- und Akteneinsichtsrecht. Ich halte es für verwunderlich, dass weder die Landesregierung noch der Landtag mir Gelegenheit gegeben haben, zu diesen spezifischen Datenschutzbelangen im Verfahrensrecht Stellung zu nehmen. Die Eingrenzung meiner Kontrollkompetenz bei der rechtsprechenden Tätigkeit, also dem richterlicher Unabhängigkeit vorbehaltenen Bereich, erklärt dieses Abweichen von der sonst üblichen Praxis nicht.

5.9 Dienstordnung für Notare

Nach Änderung der Bundesnotarordnung und anderer bundesrechtlicher Vorschriften stand auch eine Novellierung der Dienstordnung für Notare an. Bei ihrer Beteiligung durch die Justizverwaltungen konnten die Datenschutzbeauftragten in gemeinsamem Bemühen erreichen, dass die länderübergreifend geltende Ordnung an verschiedenen Punkten datenschutzfreundlicher gestaltet wurde.

So wurde angeregt, die verbreitete Praxis abzustellen, zur Identifizierung von Personen Ausweise (mit ihrem Überschuss an Daten) vollständig zu kopieren. Dem wurde im letzten Entwurf dadurch Rechnung getragen, dass nunmehr nur die schriftliche Einwilligung des Ausweisinhabers diese an sich nicht erforderliche Speicherung rechtfertigt.

Auch soll eine Verfügung von Todes wegen nur in einem verschlossenen Umschlag zur Urkundensammlung genommen werden, es sei denn die Betroffenen hätten sich mit der offenen Aufbewahrung schriftlich einverstanden erklärt.

In besonders gelagerten Ausnahmefällen soll es zum Schutz gefährdeter Beteiligter oder ihrer Haushaltsangehörigen ferner möglich sein, im Zusammenhang mit der Feststellung und Bezeichnung der Beteiligten bei der Beurkundung von einer Wohnungsangabe abzusehen. Damit lassen sich Persönlichkeitsgefährdungen vermeiden, die bis zu ganz handfesten Bedrohungen reichen können.

Zur in manchen Bundesländern - trotz der klarstellenden Entscheidung des Bundesgerichtshofs (NJW 1991, S. 568) - noch diskutierten Frage, ob Notariate der Kontrollkompetenz der Landesdatenschutzbeauftragten unterliegen, wäre eine deklaratorische Regelung in der Dienstordnung für Notare sicherlich hilfreich gewesen. Leider enthält der letzte mir vorliegende Entwurf zu dieser Frage keine Aussage. In unserem Land sieht die Praxis keine Zweifel an der Zuständigkeit.

Für die „bei Vornahme von Beurkundungen außerhalb des Amtsbereichs und der Geschäftsstellen zu beachtenden Grundsätze“ ist die Regelungs-

kompetenz nunmehr zu den Notarkammern übergewechselt. Ich habe deshalb auch bei der Saarländischen Notarkammer angeregt, Datenschutzbelange in ihre Richtlinie hierzu mit einzubeziehen. In ihr wird jetzt ausdrücklich darauf hingewiesen, dass die Umstände dieser Beurkundung außerhalb der Geschäftsstelle nicht zu einer Gefährdung der Verschwiegenheitsverpflichtung führen darf.

Damit werden einige Vorschläge zu einem verbesserten Datenschutz auch in der notariellen Tätigkeit umgesetzt.

5.10 Behandlung von Post durch Gerichte und Staatsanwaltschaft sowie Gebäudezugangssicherung

Der gerichtliche und vor allem aber auch der staatsanwaltschaftliche Postlauf bedarf, weil in diesen Stellen mit sehr sensiblen Daten umgegangen wird, einer besonders guten organisatorischen Datensicherung. Hier gibt es noch Verbesserungsbedarf.

Aus Anlass von Eingaben musste ich zu einer für die Staatsanwaltschaft und mehrere Gerichte gemeinsam handelnden Poststelle klarstellen, dass nur dann datenschutzgerecht verfahren wird, wenn hierbei die zuliefernden öffentlichen Stellen (Gerichte und Staatsanwaltschaft) jeweils eindeutig die Verantwortung für die Behandlung ihrer Post tragen. Die Tätigkeit der Poststelle ist nicht automatisch der – insofern zufälligen – organisatorischen Anbindung der Gemeinsamen Poststelle zuzurechnen. Ist die Gemeinsame Poststelle bei einer Stelle eingerichtet, findet für die andere im datenschutzrechtlichen Sinne eine Datenverarbeitung im Auftrag statt, wenn deren Post dort abgefertigt wird, bei eigenständiger Ausgestaltung der Poststelle für beide. Insofern muss jede der beteiligten Stellen (ggf. als Auftraggeberin) für die Poststelle ein Weisungsrecht dahingehend wahrnehmen, wie mit „ihren“ Daten umzugehen ist. Lässt sich dies unter Beachtung von Datenschutzmaßnahmen nicht einheitlich für alle beteiligten Stellen regeln, so ist den Besonderheiten entweder durch Einzelweisung Rechnung zu tragen oder es sind Sonderbehandlungen aus der Auftragsdatenverarbeitung herauszunehmen.

Im Zusammenhang mit den Eingaben stand hierzu fest, dass die Kuvertierung von staatsanwaltlichen Bescheiden mit sensiblem Inhalt bereits bei der Staatsanwaltschaft zu erfolgen hat, um die Kenntnisnahme unbefugter Personen möglichst zu verhindern.

In anderem Zusammenhang war die völlig unzulängliche Gebäudesicherung zu bemängeln, die ich bei einer Dienststelle vorfand. Obwohl eingeräumt wurde, durch personelle und räumliche Ausstattung seien die Risiken vermeidbar, wurden dennoch keine konkreten Abhilfemaßnahmen in Aussicht gestellt. Dabei kann es aus der Sicht des Datenschutzes nicht sein Bewen-

den haben. Das Ministerium der Justiz muss, wenn ihm solche gravierenden Mängel in der Ausstattung bekannt werden, unverzüglich für eine Änderung der Situation Sorge tragen.

5.11 Fax-Dienstanweisung bei den Gerichten

Wie schon in den Vorjahren (17. TB 3.15; 16. TB Anlage 3.14; 14. TB TZ 11.5 Anlage 10) komme ich auch in diesem Tätigkeitsbericht nicht umhin, auf Mängel bei der Telefax-Nutzung hinzuweisen, die sich mir als Auswirkung fehlender Fax-Dienstanweisungen darstellen. Bei aller Unterstützung von Deregulierungsbemühungen der Landesverwaltung, die gern den Wegfall verzichtbarer Rechts- und Verwaltungsvorschriften positiv herausstellt: offenbar können nur Fax-Dienstanweisungen den korrekten Weg weisen, was peinliche Pannen immer wieder beweisen. Im Berichtszeitraum sind, soweit die Fälle an mich herangetragen wurden, verstärkt die Gerichte durch fehlerhafte Übermittlungen per Fax auffällig geworden.

Neben den technischen Sicherungen sind es auch schlichte Vorsichtsmaßnahmen, die den Bediensteten immer wieder in Erinnerung zu rufen sind. Ersichtlich sind solche ihnen noch nicht „in Fleisch und Blut“ übergegangen, auch wenn der Gebrauch moderner Hilfsmittel immer häufiger wird. Als Hilfe für die Gerichte erscheint mir eine Muster-Dienstanweisung des Justizministeriums daher geboten. So ließe sich das Risiko sicherlich vermindern, dass unbefugte Personen im Umkreis des Adressaten oder gänzlich unzuständige Personen Kenntnis von einem Bußgeldverfahren erhalten oder über die Pfändung von Arbeitseinkommen – um nur Beispielsfälle zu nennen – informiert werden. Für die obersten Landesbehörden ist mit der Gemeinsamen Geschäftsordnung eine allgemeine Regelung bereits vorgesehen.

6 Polizei

6.1 Änderung des Saarländischen Polizeigesetzes

Herausragende Bedeutung für den Datenschutz im Polizeibereich hatte naturgemäß die Novellierung des Saarländischen Polizeigesetzes (SPolG). Entsprechend den politischen Aussagen vor der Landtagswahl hatte die neue Landesregierung zügig einen Entwurf hierfür erarbeitet und in die parlamentarischen Beratungen eingebracht. Dort erweiterten Fraktionsinitiativen den Gegenstand noch um weitere Punkte, darunter die datenschutzrechtlich relevante Videobeobachtung.

Während ein Teil der Änderungen zu begrüßen war, musste ich aus datenschutzrechtlicher Sicht den zentralen Zielsetzungen widersprechen. Mit

meinen Einwänden hiergegen fand ich aber bei der Landesregierung und im wesentlichen auch bei der Mehrheit im Landtag kein Gehör.

Eine Verschlechterung für das Recht auf informationelle Selbstbestimmung ist, dass als Schutzobjekt polizeilichen Handelns – wieder – die „öffentliche Ordnung“ eingeführt wird. Damit werden hoheitliche Eingriffe in Freiheitsrechte der Bürger auf eine undeutliche Grundlage gestützt, die für die Betroffenen wie für die ermächtigten Polizeibehörden und die Kräfte im Einsatz „vor Ort“ nicht mit der nötigen Klarheit Voraussetzungen und Umfang der Maßnahmen erkennen lassen und die auch keine parlamentarische Legitimation hat, weil es ja gerade nicht darauf ankommen soll, dass die möglicherweise verletzten Regeln in einem geordneten Verfahren, gestützt auf die Interessenabwägung der Volksvertretung, zustande gekommen sind. Zu Recht hatte das - in dieser Hinsicht vorbildlich liberale - frühere saarländische Polizeirecht Eingriffe nur zur Abwehr von Gefahren für die öffentliche Sicherheit zugelassen. Auch dieser Begriff ist ja sehr weit; er umfasst Handlungsgebote und –verbote durch jegliche Normen unserer gesamten verfassungsgemäßen Rechtsordnung, gleich welchen Rangs, und damit auch die weitgefassten Straf- und Ordnungswidrigkeitsbestimmungen, die ihrerseits als „Verstöße gegen die öffentliche Ordnung“ aufgeführt sind. Da auch sachverständige Praktiker die Entbehrlichkeit dieser Rechtsgrundlage bestätigen, habe ich den Eindruck, dass die – im Parlament nicht umstrittene - Einführung eher symbolischen Effekten als polizeilichen Erfordernissen dient.

Mit den „lagebildabhängigen Kontrollen“ wurde im Grenzstreifen von 30 km zu Frankreich und Luxemburg – also nahezu dem gesamten Land – die Schleierfahndung eingeführt, die der Vollzugspolizei erlaubt, ohne näheren Verdacht Personen anzuhalten, sich Ausweispapiere aushändigen zu lassen und Sachen in Augenschein zu nehmen, auch solche, die sich in verschlossenen Kofferräumen oder Handtaschen befinden. Dies soll zur vorbeugenden Bekämpfung der grenzüberschreitenden Kriminalität geschehen, und zwar auf Grund von Lagebildern, bei denen völlig unklar bleibt, welche Informationen diese enthalten (müssen), wie großflächig sie angelegt sind und wer die Entscheidung zum Einsatz trifft; für eine Kontrolle, mit der Betroffene die Zulässigkeit klären lassen wollen, also keine guten Bedingungen.

Von dieser Möglichkeit polizeilicher Befragung werden ganz überwiegend Personen betroffen sein, die sich nichts haben zuschulde kommen lassen. Trifft insoweit gewissermaßen bereits der Gesetzgeber faktisch die Einzelabwägung zwischen Einzelinteressen und übergeordneten Belangen, müssen also letztere von umso höherem Gewicht sein, damit sich die Betroffenen dem unterordnen müssen. Die Bekämpfung der grenzüberschreitenden Kriminalität ist auch nach meiner Auffassung eine wichtige Aufgabe. Mich hat aber nicht überzeugen können, dass dieses Instrument zu einem Zeitpunkt als unabdingbar hierfür eingeführt werden soll, zu dem nach den von

den Innenressorts selbst vorgelegten Daten diese Kriminalität in unserem Land rückläufig ist und sich insbesondere Schleusungsdelikte an andere Grenzen verlagert haben. Ich habe dies im Gesetzgebungsverfahren – vergeblich – unter Hinweis auf den Schengen-Erfahrungsbericht 1998 geltend gemacht. Der von der IMK im November 1999 verabschiedete neue Schengen-Erfahrungsbericht stellt erneut die deutlich abnehmenden Fälle an der saarländisch-französischen Grenze heraus. Problematisch sind demgegenüber Auslegungsversuche des Innenressorts, einen angeblich im Saarland feststellbaren Kriminalitätsanstieg aus in einem Jahr tatsächlich höheren Zahlen herauszulesen; diese ergaben sich daraus, dass hierbei nicht nur Tatverdächtige, sondern auch Opfer gezählt werden und in einem einzelnen Verfahren über 500 lothringische Geschädigte für den vermeintlichen Anstieg sorgten.

Als jedenfalls nötig habe ich für eine etwaige Einführung dieses Instruments klarere materielle und verfahrensmäßige Schranken verlangt:

- So erscheint nicht hinnehmbar, dass mit verdachts- und anlasslosen Kontrollen überall, also nicht nur auf Durchgangsstraßen, sondern sogar außerhalb des öffentlichen Verkehrsraums, gerechnet werden muss.
- Es bleibt unklar, welche Art und Intensität an grenzüberschreitender Kriminalität derartige Maßnahmen rechtfertigen sollen, wenn sie nicht etwa in einem Straftatenkatalog bestimmt ist und beispielsweise auf organisierte Begehungsweise eingegrenzt wird.
- Verfahrensmäßig wäre nötig, die Befugnis für die Anordnung auf die Behördenleitung einzugrenzen und zur Sicherstellung einer Überprüfung die Lagebilder zu dokumentieren, die Grundlage einer solchen Anordnung gewesen sind; die Notwendigkeit von deren Fortbestand ist sehr kurzfristig zu überprüfen. Gedacht werden könnte auch an die Einbindung des Landesbeauftragten für Datenschutz wie in § 37 Abs. 4 SPolG.
- Zur „Erfolgskontrolle“ einer solchen Befugnis sollte eine Befristung erwogen werden, wie dies etwa auch im BGS-Gesetz geschehen ist.

Das Parlament hat dies nicht für nötig gehalten. Ich habe indes Zweifel, ob die verfassungsgerichtliche Bestätigung einer im Wortlaut teilweise gleichlautenden Norm durch das Verfassungsgericht in Mecklenburg-Vorpommern ohne weiteres auf die Lage an den EU-Binnengrenzen übertragen werden kann.

Der Regierungsentwurf hatte von einem Vorschlag für eine Videoüberwachung noch abgesehen, obwohl entsprechende Forderungen in der öffentlichen Diskussion bereits früher erhoben worden waren, auch wohl deshalb, weil ein Bedarf für den Einsatz im Land aktuell nicht gesehen wurde. Auf Vorschlag einer Fraktion wurde diese Befugnis aber jedenfalls „vorsorglich“ in das Polizeigesetz eingefügt.

Danach erhält die Vollzugspolizei die Möglichkeit, an öffentlich zugänglichen Orten Bildaufzeichnungen von Personen anzufertigen, „wenn aufgrund von Tatsachen anzunehmen ist, dass dort Straftaten verabredet, vorbereitet oder verübt werden“. Auch für Verkehrs- und Versorgungsanlagen, Amtsgebäude, besonders gefährdete Objekte und deren unmittelbare Nähe sowie in öffentlichen Verkehrseinrichtungen soll dies erlaubt sein.

Ich halte zwar die Möglichkeit einer offenen Videoüberwachung öffentlich zugänglicher Orte zu eng begrenzten Zwecken nicht für gänzlich ausgeschlossen und habe dies auch mit meinen Kollegen in einer Entschließung zum Ausdruck gebracht, die als Anlage 13 abgedruckt ist. Notwendig ist indes eine präzise Umschreibung der Voraussetzungen und Modalitäten. Deshalb habe ich dies gegenüber dem ursprünglich eingebrachten Vorschlag der Fraktion eingefordert. Dem hat das Parlament – auch aufgrund der Anhörung von Praktikern und Wissenschaftlern aus anderen Ländern – teilweise entsprochen. So hat es von Tonaufzeichnungen Abstand genommen, eine Hinweispflicht auf die Überwachung und eine Löschungspflicht für Aufzeichnungen grundsätzlich nach spätestens zwei Wochen festgelegt.

Dagegen fehlt es an einer gestuften Regelung, die zwischen der „bloßen“ zeitgleichen Beobachtung – mit auch dem Ziel, unmittelbar zur Gefahrenabwehr einzugreifen – und der Aufzeichnung und damit Möglichkeit zur Weiterverarbeitung auch zu anderen Zwecken unterscheidet. Es ist nicht sichergestellt, dass die Beobachtung Teil eines Gefahrenabwehrkonzepts ist, das gerade auf diese Gefahrenabwehr zielt; insbesondere von Polizeipraktikern wird auf diese Notwendigkeit (und den hierdurch keineswegs erzielbaren Effekt deutlicher Personaleinsparungen) verwiesen. Eine Benachrichtigung identifizierter Einzelpersonen, deren Daten gespeichert bleiben, ist nicht angeordnet. Es gibt keine Vorkehrungen gegen eine – ggf. zusammen mit nichtpolizeilichen Einrichtungen – flächendeckende Kontrolle, die in jedem Fall unverhältnismäßig wäre. Verzichtet wurde auch auf eine zunächst nur befristete Einführung dieses Instruments, um dem Gesetzgeber eine Erfolgskontrolle nahe zu legen.

Vorläufig ist noch nicht erkennbar, auf welche Örtlichkeit sich der Einsatz dieser gesetzlichen Möglichkeit richten soll. Sofern er bevorsteht, werde ich selbstverständlich bei der gebotenen Beteiligung des LfD an der Einrichtung und bei der Kontrolle darauf achten, dass Datenschutzbelange so weit wie möglich gewahrt bleiben.

6.2 Erlass über die Meldung wichtiger Ereignisse (WE-Meldung)

Um die Information der Einsatzleitung und ggf. der politischen Führung in bedeutsamen Fällen sicherzustellen, gibt es in der Polizei spezielle Meldungen. Je nach Anlass werden die Meldewege hierfür in dem ministeriellen „Erlass über die Meldung wichtiger Ereignisse (WE-Meldung) und die Be-

nachrichtigung der Staatsanwaltschaft in Strafsachen durch die Behörden und Einrichtungen der Vollzugspolizei“ bestimmt. Aus Anlass einer Eingabe habe ich die Vorschrift und die praktische Vorgehensweise der Polizei überprüft.

Festzustellen war zum einen, dass die Dienststellen der Vollzugspolizei recht unterschiedliche Einschätzungen über die Wichtigkeit eines Ereignisses zugrundegelegt haben, das gemeldet wurde. Zum anderen sind sie ihrer Meldepflicht teilweise recht konkret durch Übermittlung personenbezogener Daten u.a. an das Ministerium des Innern (Lagezentrum) nachgekommen; diese Stelle im Ministerium war nach dem Erlass stets mit zu benachrichtigen.

Auch innerhalb der Polizei darf es keinen umfassenden Datenfluss geben. Wenn personenbezogene Meldungen an Stellen außerhalb der sachbearbeitenden Dienststelle gehen, so bedürfen diese als Datenübermittlungen einer gesetzlichen Grundlage, in der die Erforderlichkeit der Datenübermittlung und deren Zweckbestimmung für den Empfänger zum Ausdruck kommt. Die in diesem Zusammenhang in Betracht zu ziehende Wahrnehmung von Aufsichts- und Kontrollbefugnissen durch das Ministerium des Innern setzt auch in Fällen wichtiger Ereignisse im Polizeibereich nicht zwingend eine personenbezogene Schilderung des Ereignisses voraus.

In erster Linie habe ich empfohlen, nach dem Grundsatz der Datensparsamkeit, die Übermittlung personenbezogener Daten so weit wie möglich zu vermeiden. So ist es beispielsweise bei einem größeren Verkehrsunfall als mitzuteilendem wichtigem Ereignis im Regelfall nicht erforderlich, die Insassen der beteiligten Fahrzeuge namentlich aufzuführen und dies auch dem Ministerium bekannt zu geben. Für die Entbehrlichkeit dieser Angaben spricht die bisherige Praxis einer Polizeidirektion, wo auf die konkrete Angabe von personenbezogenen Daten bereits verzichtet wird.

Ein weiterer Regelungsgegenstand in dem Erlass betraf Mitteilungen über Ereignisse mit Beteiligung von Polizeibediensteten. Solche personenbezogenen Angaben mussten sowohl hinsichtlich des Zeitpunktes (im unmittelbaren Anschluss an das Ereignis) als auch des Adressaten (Ministerium des Innern, Lagezentrum) problematisch erscheinen.

Denn soweit es um den Verdacht einer Straftat geht, ist nach Nr. 15 der Anordnung über Mitteilungen in Strafsachen (MiStra) erst zu den dort angegebenen Zeitpunkten (z.B. Anklageerhebung) eine Mitteilung an den Dienstherrn zu richten, die auch nicht von Seiten der Polizei angeordnet werden darf, sondern durch die Staatsanwaltschaft oder zu einem späteren Zeitpunkt durch das Gericht. Daneben bestehende Vorab-Übermittlungen sind stets dann als bedenklich anzusehen, wenn der Zweck und die Erforderlich-

keit der Übermittlung an die bezeichnete Stelle im Ministerium als Adressaten und die entsprechende Rechtsgrundlage im Unklaren bleibt.

Zur Gefahrenabwehr kann eine Vorab-Information des Ministeriums allenfalls dann erfolgen, wenn das Verhalten eines Polizeibediensteten eine Gefahr darstellt, die ihn beispielsweise als Waffenträger ungeeignet erscheinen lässt. Sobald jedoch der Verdacht einer Straftat besteht, handelt es sich auch dann um Daten aus dem Strafverfahren, deren Übermittlung auf der Grundlage des Saarländischen Polizeigesetzes der Zustimmung der für die Ermittlung zuständigen Staatsanwaltschaft bedarf (§ 32 Abs. 1 Satz 3 SPolG). Eine bloße Benachrichtigung an Stelle der Zustimmung – wie im Erlass vorgesehen – reicht für die parallele Datenübermittlung insofern nicht aus.

In den übrigen Fällen müssen - mangels anderer Rechtsgrundlagen - die im Justizmitteilungsgesetz i.V.m. der MiStra angegebenen Zeitpunkte auch für Polizeibedienstete beachtet werden.

Wie mir das Ministerium des Innern mitgeteilt hat, sollen die Meldewege überdacht und die bevorstehende Änderung der Organisationsstruktur der Polizei berücksichtigt werden. Für die Neufassung des Erlasses, der mir vorgelegt werden soll, lege ich auch Wert auf die Festlegung eines engen Adressatenkreises, der auch in der Lage ist, notwendige Maßnahmen zu veranlassen, und auf die Bestimmung kurzer Aufbewahrungsfristen, die bislang im Erlass noch fehlen.

6.3 Polizeiliche Beobachtung; Neufassung des Landesteils der Polizeidienstvorschrift

Das Ministerium des Innern hatte mir bereits im Jahre 1998 die Polizeidienstvorschrift „Polizeiliche Beobachtung“ (Neufassung des Landesteils) zur Stellungnahme zugeleitet. Auffallend war in diesem Zusammenhang die Bestimmung zur polizeilichen Beobachtung im Saarländischen Polizeigesetz (§ 29 Abs. 1 Nr. 2), die weitgehend gleichlautend ist mit einer Norm im Sächsischen Polizeigesetz.

Der dortige Verfassungsgerichtshof hatte diese schon 1996 für nichtig erklärt; in der Entscheidung wurde ein Defizit an Normenklarheit und Bestimmtheit gerügt. An diesem Mangel leidet auch die entsprechende Norm des Saarländischen Polizeigesetzes: so können nach dessen Wortlaut ehemalige Straftäter polizeilich beobachtet werden, wenn die Gesamtwürdigung der Person und ihre bisherigen Straftaten erwarten lassen, dass sie auch künftig Straftaten von erheblicher Bedeutung begehen werden.

Zumindest für die das Gesetz konkretisierende Polizeidienstvorschrift ist eine verfassungskonforme Auslegung dieser Norm zu fordern. Hieran fehlt

es noch; ich habe auf die Entscheidung des Verfassungsgerichts ausdrücklich hingewiesen.

Der verfassungsrechtliche Bestimmtheitsgrundsatz erfordert nach den Ausführungen des Sächsischen Verfassungsgerichtshofs eine Negativprognose für den ehemaligen Straftäter, die nicht nur auf der Grundlage von Erfahrungswissen und Vermutungen getroffen wurde, sondern durch objektive Umstände wie Tatsachen oder wenigstens tatsächliche Anhaltspunkte für zukünftiges Handeln untermauert sein muss. Eine noch höhere Eingriffsschwelle für die polizeiliche Beobachtung, die ja verdeckt und nicht offen abläuft, ist für ehemalige Straftäter zu verlangen, denn sie muss auch dem Resozialisierungsgedanken Rechnung tragen.

Es sollten in den bundesweiten Beobachtungsdateien der Polizei nur solche ehemaligen Straftäter enthalten sein, für die aufgrund nachvollziehbarer Momente die Verwendung des Begriffs „gefährlicher Intensivtäter“ angemessen erscheint.

Eine dahingehende Konkretisierung und Neufassung der Polizeidienstvorschrift ist mir bislang nicht vorgelegt worden.

6.4 Polizeiliche Beobachtung im Rahmen der Strafverfolgung

Auch im Bereich der Strafverfolgung kommt polizeiliche Beobachtung in Betracht. Im Gegensatz zur präventiven polizeilichen Beobachtung im Polizeirecht ist auf der Grundlage der Strafprozessordnung (§ 163e) nicht nur eine Beobachtung von Verdächtigten, sondern auch von deren möglichen Kontaktpersonen zulässig. Die Anordnung wird in bundesweite polizeiliche Dateien zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes des Täters eingestellt.

Eine derartige Maßnahme im repressiven Bereich wurde anlässlich einer Eingabe überprüft. Meine Überprüfung hat im konkreten Fall die grundsätzliche Zulässigkeit der Maßnahme in der Vergangenheit ergeben, wenngleich letzte Zweifel im Hinblick auf die Speicherungsdauer der Daten des Petenten nicht ausgeräumt werden konnten, weil die Daten aufgrund seiner Intervention vor dem Zeitpunkt der Eingabe bereits beim Bundeskriminalamt gelöscht worden waren.

6.5 Speicherungsumfang in "INPOL-neu"

Das aktuelle Datenaustauschsystem "INPOL" der Polizeien des Bundes und der Länder wird seit geraumer Zeit fortentwickelt und soll demnächst als "INPOL-neu" im Bund und den Ländern installiert werden.

Mit den verbesserten technischen Möglichkeiten gehen auch polizeiliche Bestrebungen einher, die Zusammenarbeit über die bestehende rechtliche

Zulässigkeit hinaus zu verbessern. Zu diesen Vorstellungen haben sich die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung besorgt darüber geäußert, dass entgegen den Bestimmungen im Bundeskriminalamtsgesetz auch Daten zu Straftaten, die bisher nur regional gespeichert werden dürfen, in den Bundes-Kriminalaktennachweis übernommen werden sollen (Anlage 18). Die geltenden gesetzlichen Bestimmungen sind auch Ausdruck des Verhältnismäßigkeitsgebotes, wonach personenbezogene Daten über Straftäter nicht über deren Wirkungskreis und Bedeutung im Einzelfall hinaus gestreut werden sollen.

An die Innenressorts des Bundes und der Länder richtete sich daher die Aufforderung, von der geschilderten Erweiterung des Bundes-Kriminalaktennachweises abzusehen.

6.6 Auftragsdatenverarbeitung durch das Bundeskriminalamt

Die Verhütung und Verfolgung von Straftaten ist sowohl Aufgabe der Polizeien der Länder als auch des Bundeskriminalamtes (BKA). In die Kompetenz des Bundeskriminalamtes fällt die Informationssammlung über Straftaten von länderübergreifender, internationaler oder erheblicher Bedeutung. Straftaten, die diese Voraussetzungen nicht erfüllen, also insbesondere solche von rein regionaler Bedeutung, werden lediglich von den Landeskriminalämtern gesammelt und ausgewertet und auf Landesebene gespeichert.

Das Saarland hatte bereits 1984 ein Verwaltungsabkommen über die Nutzung der Datenverarbeitungskapazitäten des Bundeskriminalamtes durch die Polizei für seine Landesdatenhaltung abgeschlossen. Dabei handelte es sich im Hinblick auf die allein auf Landesebene zu speichernden Daten nach datenschutzrechtlichen Kriterien um eine Auftragsdatenverarbeitung, die der Auftragnehmer (BKA) nach Weisung des Saarlandes (Auftraggeber) durchzuführen hatte. In der Vergangenheit war der Datenschutzaspekt nur unzureichend im Bewusstsein der Landespolizei, nach Inkrafttreten des BKA-Gesetzes aus dem Jahre 1997 wurde vor allem die Frage aufgeworfen, ob nicht nur eine befristete, sondern eine dauerhafte Datenverarbeitung im Auftrag nach der nunmehr vorhandenen Rechtsgrundlage zulässig sei.

Mit einer Entschließung haben die Datenschutzbeauftragten des Bundes und der Länder ihre Bedenken gegen einer dauerhafte Datenverarbeitung der Landesdaten beim BKA geäußert (Anlage 19).

Für die nach Auffassung der Innenminister des Bundes und der Länder auch dauerhaft zulässige Auftragsdatenverarbeitung der Länder beim BKA wurde eine Rahmenvereinbarung mit datenschutzrechtlichen Regelungen erstellt, der sich auch das Saarland bei einer auch zukünftig dauerhaften Auftragsdatenverarbeitung im Hinblick auf den vertraglichen Datenschutzgehalt anzuschließen hätte.

Zwischenzeitlich hat mir aber das Innenministerium mitgeteilt, dass im Saarland die Auftragsdatenverarbeitung beim BKA zum 31.12.2000 beendet wurde.

6.7 Auskunftsersuchen bei verdeckten Maßnahmen der Polizei

Mit Auskünften, die Betroffene von der Polizei oder mittelbar von mir erhalten, wenn sie sich an mich wegen eines möglichen Datenschutzverstoßes wenden, sind diese oft nicht zufrieden, gerade dann nicht, wenn die Auskunftsersuchen sich auf – meist nur vermutete – Telefonüberwachungen oder andere verdeckte Maßnahmen der Polizei beziehen. Hier sind aber auch für den LfD gesetzliche Besonderheiten zu beachten, die nicht immer auf das Verständnis der Auskunftsbegehrenden stoßen.

Sowohl bei repressiven als auch bei präventiven Maßnahmen der Polizei ist nicht von der Hand zu weisen, dass eine Auskunft geeignet ist, den verdeckten Charakter der Maßnahme zunichte zu machen. Der Leitende Oberstaatsanwalt, mit dem ich die Thematik erörtert habe, hat insofern zu Recht darauf hingewiesen, dass für inhaltliche Auskünfte im repressiven Bereich der Zeitpunkt maßgeblich sein muss, der von der Strafprozessordnung für die Benachrichtigung des Betroffenen (§ 101 StPO) angeordnet ist: die Beteiligten sind zu benachrichtigen, sobald dies ohne Gefährdung des Untersuchungszwecks der öffentlichen Sicherheit, von Leib oder Leben einer Person sowie der Möglichkeit der weiteren Verwendung eines eingesetzten nicht offen ermittelnden Beamten geschehen kann.

Diese Rechtslage wird im allgemeinen Datenschutzrecht durch die Bestimmung ergänzt, wonach bei Daten, die von Sicherheitsbehörden stammen, Auskünfte an die Zustimmung dieser Behörden gebunden sind, wenn sie eine solche Herkunft erkennen lassen (§ 18 Abs. 5 SDSG).

An diese Gesetzeslage ist der LfD selbstverständlich gebunden. Auch die Mitteilung durch ihn darf keine Rückschlüsse auf den Erkenntnisstand der speichernden Stelle zulassen, sofern nicht deren ausdrückliche Zustimmung vorliegt (§ 2 Abs. 1 Satz 2 letzter HS i.V.m. § 19 Abs. 6 BDSG).

Probleme sieht die Staatsanwaltschaft allerdings bei der Beantwortung von Anfragen durch den LfD dann, wenn es bei der Polizei oder Staatsanwaltschaft gar keine gespeicherten Daten gibt und mithin auch keine Stelle vorhanden ist, die einer Auskunft zustimmen könnte. Sie befürchtet bei Weitergabe der datenschutzrechtlich korrekten (Negativ)-Auskunft, dass nichts gespeichert sei, unter Umständen Rückschlüsse bei dem Petenten über ihren Erkenntnisstand und ihre Maßnahmen; solche Anfragen könnten auch gezielt die Aussage „herauslocken“ wollen, dass verdeckte Maßnahmen eben nicht durchgeführt werden. Ob eine derartige „Ausforschungsanfrage“ überhaupt realistisch ist, mag zweifelhaft sein. Der mögliche Rückschluss

ergäbe sich indes nur im Vergleich zur Antwort in den oben genannten Fällen, in denen berechtigterweise eine wahrheitsgemäße Sachauskunft nicht gegeben werden muss. Auch der unmittelbar bei Staatsanwaltschaft oder Polizei gestellte datenschutzrechtlichen Auskunftsanspruch kann aber nicht generell abgelehnt werden, sondern nur dann, wenn bei dem betreffenden Petenten Anhaltspunkte für eine Gefährdung von Sicherheitsinteressen belegt sind. Inwieweit bei einer mittelbaren Auskunft durch den LfD den Bedenken der Staatsanwaltschaft durch besondere Formulierungen Rechnung getragen werden muss, wäre mit ihr anhand eines konkreten Einzelfalls erneut zu erörtern.

6.8 Richtlinien für die polizeiliche Verkehrsüberwachung (VÜ-RiLi)

Zum 1.1.2000 hat das Ministerium für Inneres und Sport Richtlinien für die polizeiliche Verkehrsüberwachung in vorläufiger Fassung in Kraft gesetzt.

Hätte mich das Ministerium vor der Inkraftsetzung als Verwaltungsvorschrift beteiligt, wie es gemäß § 8 Abs. 1 Satz 2 SDSG geboten gewesen wäre, hätte ich aus Sicht des Datenschutzes bereits damals Stellung nehmen können. Positiv hätte ich vermerkt, dass in der VÜ-RiLi alle bisher geltenden Erlasse, Dienstanweisungen und Richtlinien, einschließlich der mit dem Landesbeauftragten erarbeiteten Kriterien, nunmehr zusammengefasst sind.

Kritisch konnte ich mich so erst nachträglich zur Formulierung der Leitgedanken zur polizeilichen Verkehrsüberwachung äußern. Dort wird nämlich besonders das „Prinzip der ganzheitlichen Kontrolle“ betont, an dem sich die Überwachung wesentlich auszurichten hat. Das bedeutet, dass neben verkehrsrechtlichen Gesichtspunkten auch allgemeinpolizeiliche Aspekte betrachtet und entsprechende umfassende Maßnahmen getroffen werden.

Ganzheitliche Kontrolle darf nur ein Nebenprodukt der Verkehrsüberwachung sein, nicht jedoch ihr primärer Zweck und eigentlicher Grund für das polizeiliche Einschreiten ohne verkehrsspezifischen Anlass. Zunächst muss vielmehr Grund für die Verkehrsüberwachung auf der entsprechenden Rechtsgrundlage gegeben sein, damit im Rahmen der Verkehrskontrolle auch ganzheitliches polizeiliches Kontrollieren zum Zuge kommen darf. Soweit sich dies im Rahmen des Opportunitätsprinzips und selbstverständlich auch des Legalitätsprinzips bewegt, bestehen allerdings hiergegen dann keine Bedenken.

Bei der Erarbeitung der endgültigen Fassung wären etwaige Missverständnisse zum Passus „Prinzip der ganzheitlichen Kontrolle“ auszuräumen.

6.9 Anfertigung von Lichtbildern im ruhenden Straßenverkehr

In einer Eingabe wurde die Frage gestellt, ob ein Hilfspolizeibeamter, der ausschließlich für den ruhenden Verkehr zuständig ist, Lichtbilder von "Parksündern" anfertigen darf. Sein Vorgehen hatte den Eindruck erweckt, mit der Fotografie wolle er nicht nur die Parksituation dokumentieren, sondern auch die Identität des Fahrzeugführers, der im Moment der Aufnahme gerade dabei war, sein Fahrzeug wegzufahren.

Dass dies nicht in der Absicht des Hilfspolizeibeamten lag, ergab sich im anschließenden Bußgeldverfahren, da der Hilfspolizeibeamte eine Frau als Halterin zur Kasse bitten wollte, obwohl auf dem Foto eindeutig ein Mann abgebildet war.

In der Erörterung mit dem Hilfspolizeibeamten ging es um die Rechtmäßigkeit des Anfertigens von Lichtbildern im ruhenden Verkehr und vor allem um die Vernichtung des angefertigten Fotos, auf dem der Petent deutlich zu erkennen war.

Grundsätzlich vertrete ich die Auffassung, dass das Anfertigen von Lichtbildern von Personen, die einer Ordnungswidrigkeit im ruhenden Verkehr verdächtigt werden, eine unverhältnismäßige Maßnahme darstellt; § 100 c StPO halte ich hier nicht für anwendbar. Fotografien als polizeiliche erkennungsdienstliche Maßnahmen sollten in diesen Bagatellfällen nicht in Betracht gezogen werden. Dagegen bestehen gegen die Dokumentation der Beschilderung, der jeweiligen Verkehrssituation sowie des Fahrzeugstandortes durch ein Foto keine datenschutzrechtlichen Bedenken. Zufällig auf dem Foto befindliche erkennbare Personen, wie z. B. Passanten, Fahrer anderer Fahrzeuge, sind jedoch unkenntlich zu machen.

Nachdem im konkreten Fall die Ordnungswidrigkeit im ruhenden Verkehr wegen Verjährung nicht mehr gegenüber dem Fahrzeugführer verfolgt werden konnte, wurde die Fotografie vernichtet. Zurück blieben allerdings Zweifel, ob für die datenschutzrechtliche Position ausreichend Verständnis geweckt werden konnte.

6.10 Demonstration

Bei Zusammenkünften mehrerer Personen wird es gewöhnlich nicht geschätzt, wenn staatliche Organe der Polizei oder des Verfassungsschutzes anwesend sind, beobachten oder sogar augenfällig einschreiten. In der Bevölkerung kommt bei solchen Anlässen, vor allem wenn sie ihr Grundrecht auf "Demonstrationsfreiheit" nach Art. 8 Grundgesetz wahrnehmen, schnell die Befürchtung auf, hier werde unzulässig von Seiten des Staates beobachtet und Personen registriert, damit sie von ihren Freiheitsrechten nur sparsam oder auch gar nicht mehr Gebrauch machen.

Natürlich dürfen die Sicherheitsbehörden nur im Rahmen ihrer normierten Befugnisse und nur zu dem Zweck tätig werden, ihre festgelegten Aufgaben zu erfüllen. Dass sie aber ihre Funktion wahrnehmen, muss zum Schutz der Allgemeinheit und der Rechte Dritter ebenfalls erwartet werden. Soweit dabei Informationsverarbeitung stattfindet, zielt Datenschutz nicht darauf, dies zu verhindern, sondern dafür zu sorgen, dass Bürger zu Recht Vertrauen auf die korrekte Arbeit haben können.

Im Zusammenhang mit einer Demonstration von Ausländern habe ich daher einen besorgten Petenten auf die Befugnisse der Polizei nach dem Versammlungsgesetz des Bundes und dem Polizeirecht des Saarlandes hingewiesen. Nach der damals noch geltenden Fassung des Polizeigesetzes waren Aufzeichnungen zur vorbeugenden Bekämpfung von Straftaten möglich; gesetzlich vorgesehen war, dass Aufzeichnungen der Polizei unverzüglich bzw. spätestens nach zwei Monaten zu löschen sind, soweit sie nicht zur Verfolgung von Straftaten oder von Ordnungswidrigkeiten von erheblicher Bedeutung erforderlich sind. Mit der letzten Novellierung einzelner Bestimmungen des Polizeigesetzes ist allerdings diese zu weitgehende Befugnis zu Recht in Übereinstimmung mit der - engeren – Norm des Versammlungsgesetzes gebracht worden.

6.11 Gewalttäter Sport

Das Saarland hat sich aufgrund zunehmender gewalttätiger Auseinandersetzungen bei Fußballspielen im Jahre 2000 ebenfalls entschlossen, am Übergangsbetrieb des Verfahrens "Gewalttäter Sport" teilzunehmen. Dazu wurden im ersten Anlauf circa 60 Personen in die im überregionalen Verbund abrufbare Datei eingestellt, bei denen die Polizei mit gewalttätigen Auseinandersetzungen aus Anlass von Fußballspielen rechnete.

Im Anschluss an Überprüfungen, die ich hierzu vorgenommen habe, hat die Polizei einige Personen, bei denen keine konkreten Anhaltspunkte für die Begehung künftiger Straftaten an Hand von im Saarland geführten Akten vorlagen, aus der Datei gelöscht. Nach eigenen Angaben der Polizei sind auch auf meinen Hinweis keine Personen mehr eingestellt, gegen die lediglich ein Platzverweis ergangen ist oder deren Personalien festgestellt wurden, ohne dass weitere Maßnahmen zu ergreifen waren.

Auf die Beschwerde eines Fußballfans habe ich mir erneut die Vorgehensweise der Polizei bei Fußballspielen eingehend darstellen lassen. Der Petent war empört darüber, dass er – wie alle anderen in einem Bus anreisenden Fans - von der Polizei bei seiner Ankunft nach mitgeführten Gegenständen durchsucht und auf seine Identität überprüft worden war, wobei auch Videoaufnahmen gefertigt wurden. Ob insbesondere die generelle Identitätskontrolle mittels Video verhältnismäßig war, erschien doch fraglich.

Die Einsatzleitung hatte polizeiliche Informationen im Bundesland eingeholt, aus dem die gegnerische Fußballmannschaft stammte. Ihr waren die Anreisenden als gewaltbereite Fans angekündigt worden, wobei aber nicht ausgeschlossen wurde, dass auch friedliche Veranstaltungsteilnehmer sich in diesem Bus hätten befinden können.

In dieser Situation ließ der Wortlaut der damals geltenden Bestimmung zur Datenerhebung bei Veranstaltungen der Polizei in der Tat einen weiten Handlungsspielraum. Zum Zeitpunkt der Prüfung hatte der Landtag zwar schon eine Norm im Polizeigesetz verabschiedet, die die Möglichkeiten eines Videoeinsatzes bei Veranstaltungen präziser (und einschränkender) regelt; sie wurde im Berichtszeitraum aber noch nicht verkündet und konnte auch nicht selbstverständlich als Auslegungshilfe für die alte Bestimmung herangezogen werden. Auf deren Grundlage musste ich konzedieren, dass es angesichts der damaligen Gefahrenprognose, die auch die Abwehr einer einfachen Gefahr zuließ, vertretbar war, die Maßnahmen als erforderlich und noch verhältnismäßig anzusehen.

Auf die zukünftig geltende Bestimmung des Polizeirechts habe ich jedoch hingewiesen. Danach sind - in Anlehnung an das Versammlungsgesetz des Bundes - gezielte Bildaufzeichnungen bei solchen Veranstaltungen nur noch bei Personen erlaubt, bei denen tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass sie Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung begehen werden. In Zukunft ist daher eine andere Vorgehensweise und Zusammenarbeit der Polizeien der Länder verlangt, damit nur solche Personen herausgegriffen werden, von denen zu erwarten ist, dass sie nicht friedlich an einer Veranstaltung teilnehmen werden. Entsprechende Zurückhaltung wurde von Seiten der Polizei in Aussicht gestellt.

Ein weiterer Anlass zur Überprüfung ergab sich im Vorfeld der Fußballeuropameisterschaft 2000. Mehrere Bundesländer – so auch das Saarland - hatten gegen Personen, die als "gewalttätige Fans" eingestuft waren, Ausreiseverbote und Meldeauflagen erlassen und den Grenzschutz hiervon unterrichtet. Nach meiner Auffassung war die zuständige Grenzschutzdirektion zwar über das Ausreiseverbot zu informieren, da sie dieses bei einem versuchten Grenzübertritt zu kontrollieren hatte, nicht jedoch über eine Meldeauflage, deren Vollzug von der örtlichen Polizei zu überprüfen war. Wenn die Behörde die Maßnahmen (Ausreiseverbot und Meldeauflage) wie im Regelfall sinnvollerweise koppelt, ist die Benachrichtigung der Grenzschutzdirektion über das Ausreiseverbot selbstverständlich zulässig.

Zu bemängeln war jedenfalls die Übermittlung einer (isolierten) Meldeauflage für den Betroffenen an die Grenzschutzdirektion ohne die gleichzeitige Verhängung eines Ausreiseverbotes, denn für die Meldeauflage fiel der Vollzug ausschließlich in die Überwachungskompetenz der Polizei, zumal der

Betroffene angesichts der Grenznähe des Saarlandes zu Frankreich ohne Verstoß gegen die Meldeauflage die Grenze kurzfristig passieren konnte.

Als gravierend bei dem Versuch, die Meldeauflage von der Grenzschutzdirektion durchsetzen zu lassen, war die Tatsache anzusehen, dass der Betroffene von dem faktischen Ausreiseverbot keine Kenntnis erhalten hatte. Es handelte sich jedoch um einen Einzelfall, dessen Wiederholung ich nicht erwarte. Die zuständige Ortspolizeibehörde ging hierbei nämlich irrtümlich davon aus, sie könne kein Ausreiseverbot erlassen, weil der Betroffene nicht im Besitz eines Passes oder Personalausweises gewesen sei. Ich habe sie gebeten, solche Fehler zukünftig zu vermeiden.

6.12 Enfopol

Auch im Sicherheitsbereich gibt es auf europäischer Ebene Überlegungen und Absprachen, mit denen entscheidende Weichen für die rechtliche und technologische Entwicklung der Telekommunikation gestellt werden. Wegen deren herausragender Bedeutung für Wirtschaft und Gesellschaft ist aber nicht hinnehmbar, dass aus einer Sicht unverrückbare Festlegungen getroffen werden, ohne dass die Wirkungen ausreichend berücksichtigt werden können.

Weil sie diese Gefahr bei den Planungen des Rates der EU zur grenzüberschreitenden Überwachung der Telekommunikation und der Internet-Nutzung (Enfopol) sahen, die seinerzeit nahezu unbemerkt erfolgten, haben die Datenschutzbeauftragten des Bundes und der Länder mit einer Entschließung einen Anstoß zu dieser Diskussion geben wollen (Anlage 4).

Schon in einem frühen Stadium ist darauf aufmerksam zu machen, dass erreichte Standards zur Wahrung des Rechts auf informationelle Selbstbestimmung bei internationaler Zusammenarbeit nicht gänzlich über Bord geworfen werden dürfen, um erstrebenswerte Ziele zu erreichen. Beim Einsatz von prepaid cards bleiben die Nutzer beispielsweise weitgehend anonym. Solche datenschutzfreundlichen Technologien sollten nicht einer perfekten Überwachung der Telekommunikation und des Internets zum Opfer fallen, auch wenn die nationalen Grenzen überschritten werden müssen und Übereinkommen mit anderen Staaten zu erzielen sind.

An der Diskussion über das Ausmaß der Erreichbarkeit von Sicherheit, aber auch gleichzeitiger Freiheit des Einzelnen werden sich die Datenschutzbeauftragten ihrer Aufgabe entsprechend beteiligen.

7 Verfassungsschutz

7.1 Abgrenzung der Zuständigkeiten zwischen G 10 Kommission und den Datenschutzbeauftragten

Das Bundesverfassungsgericht hat im Jahre 1999 in einer grundlegenden Entscheidung Leitlinien für die Befugnisse des Bundesnachrichtendienstes bei der Telefonüberwachung aufgestellt, die 1994 im sogenannten Verbrechensbekämpfungsgesetz erweitert worden waren.

Aus dieser Entscheidung lassen sich über die konkreten Verfassungsbeschwerden hinaus Grundsätze ableiten, die in Neufassungen der G 10-Gesetze des Bundes und der Länder einfließen müssen. Welche Anforderungen im Einzelnen umzusetzen sind, haben die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung dargestellt (Anlage 16). Einer der zentralen Punkte besteht in der lückenlosen Kontrolle der Abhörmaßnahmen nach dem G 10-Gesetz, das die Einschränkung des Brief-, Post- und Fernmeldegeheimnisses nach Art. 10 GG regelt.

Auch nach dem Wortlaut des saarländischen Durchführungsgesetzes zum G10-Gesetz erscheint die Kontrolle durch die G 10-Kommission nicht umfassend gewährleistet, worauf ich schon frühzeitig bei der Datenverarbeitung des Verfassungsschutzamtes im G 10-Bereich hingewiesen habe. In der Neufassung des Durchführungsgesetzes wird auf diesen Punkt ein besonderes Augenmerk zu legen sein. Keineswegs belanglos ist - gemessen an der Praxis - auch der verfassungsgerichtliche Hinweis auf die angemessene personelle und sachliche Ausstattung der Stellen, die eine lückenlose Kontrolle des G 10-Bereichs und der von dort – ausdrücklich als solche gekennzeichnet – in andere Bereiche fließenden Daten zu gewährleisten haben.

7.2 Datenverarbeitung beim Landesamt für Verfassungsschutz

Schon bei einer früheren Kontrolle hatte ich festgestellt, dass das im Verfassungsschutzamt eingesetzte interne Datenverarbeitungssystem von Anfang an nicht zufriedenstellend konzipiert war. Ganz erhebliche Mängel weist es auch im Hinblick auf die Möglichkeit der Datenschutzkontrolle auf; sie haben sich im Laufe der Jahre noch verfestigt. Hier wurde für das Jahr 2001 eine Abhilfe angekündigt, die keineswegs länger hinausgeschoben werden darf. Eine wirksame Kontrolle setzt vor allem eine Dokumentation der Datenverarbeitungsaktivitäten voraus, die Erzeugung von überprüfbaren Protokolldateien dürfte somit die Grundvoraussetzung eines automatisierten Datenverarbeitungssystems sein, worauf bei jeder Neukonzeption in erster Linie zu achten wäre.

Die Organisation bei der Aufbewahrung bzw. Speicherung muss ebenfalls verbessert werden. Löschungen sind entsprechend den vorhandenen

Dienstanweisungen vorzunehmen; auch diese sind systemseitig durch Wiedervorlagefristen zu unterstützen. Zwar ist es grundsätzlich zu begrüßen, wenn Akten zu Einzelpersonen nicht mehr getrennt neben Sachakten geführt werden. Konsequenz daraus darf jedoch nicht sein, dass die Einzelperson in der Sachakte über die zulässige Speicherfrist hinaus, sogar über Jahrzehnte, festgehalten werden, ohne dass in einem längeren Zeitabschnitt der nahen Vergangenheit Aktivitäten dieser Einzelperson zu verzeichnen gewesen wären. Sachakten, die nunmehr alle personenbezogenen Daten enthalten, sind daher nach den gesetzlich oder nach den in Dienstanweisungen vorgegebenen Fristen vom Verfassungsschutzamt selbst zu überprüfen und zu vernichten. Wenn dies nicht möglich ist, sind zumindest in dem gebotenen Umfang Schwärzungen vorzunehmen. Der Wegfall der Personenakten darf nicht dazu führen, dass Löschungsfristen leer laufen.

8 Kommunen

8.1 Behandlung personenbezogener Daten in kommunalen Gremien

Bereits in meinem letzten Bericht (TZ 6.2) war ich auf darauf eingegangen, dass in kommunalen Gremien personenbezogene Daten verschiedentlich nicht so vertraulich behandelt werden, wie dies notwendig ist. In einem Merkblatt, das ich nach der Kommunalwahl zur Unterrichtung der neugewählten Mitglieder und der Verwaltungen versandt hatte, hatte ich einige Grundsätze formuliert und Anwendungsbeispiele gegeben.

Vor einem Kreistag, dessen Vorsitzender mich darum gebeten hatte, habe ich diese Grundprinzipien erläutert und vor allem das Augenmerk und den datenschutzrechtlichen Regelungsbedarf auf Punkte gelenkt, bei denen sich wiederholt Mängel und Unklarheiten gezeigt haben. Dazu zählen insbesondere:

- Einladung, Sitzungsvorbereitung
- Behandlung von Unterlagen durch Verwaltung und Mitglieder
- Niederschriften (Tonbandprotokoll zur Erstellung der Niederschriften, Presseveröffentlichungen; Einsichtsrecht von Bürgern, von Mitgliedern)
- Personalangelegenheiten
- Rechte der Gremienmitglieder (Informationsrecht, insb. Akteneinsicht; Beachtung des Steuer-, Sozialgeheimnisses)

Als zentraler Gesichtspunkt hat sich bei jeder Fragestellung die Erforderlichkeit eines Personenbezuges herauskristallisiert, die in einzelnen Fällen doch zu sehr vernachlässigt wurde. In der Praxis wird eher darauf abgestellt, ob

der Personenbezug für viele Gremienmitglieder vielleicht von Interesse sein könnte.

In die von kommunalen Gremien zu erstellenden Geschäftsordnungen hatten datenschutzrechtliche Aspekte bislang kaum Eingang gefunden. Dankenswerterweise hat mich der Landrat des Saarpfalzkreises bei der anstehenden Überarbeitung der Geschäftsordnung des Kreistages beteiligt. Gemeinsam mit der Verwaltung und mit den aufgeschlossenen Mitgliedern des Kreistages gelang es, diese Geschäftsordnung aus meiner Sicht angemessen anzupassen bzw. zu ergänzen. Mit Zustimmung des Kreistages habe ich sie als Muster an den Stadtverband und die anderen Kreise versandt.

Eine gleiche Muster-Geschäftsordnung erarbeite ich derzeit in Kooperation mit einer Gemeindeverwaltung. Wenn es gelingt, auch diese Geschäftsordnung aus datenschutzrechtlicher Sicht angemessen aufzubereiten, werde ich sie gerne den Städten und Gemeinden als Muster zur Umsetzung übersenden.

8.2 Beschwerde über den Ortsrat einer Gemeinde

Man kann sicherlich davon ausgehen, dass die Ortsräte sich besonders der Bevölkerung ihres Ortsteils verbunden fühlen, und man kann diese Nähe auch als Teil ihrer Aufgabe ansehen. Das darf jedoch nicht dazu führen, dass persönliche Anliegen der Einwohner weniger vertraulich behandelt werden, als es gesetzlich vorgeschrieben ist.

Zu Recht beschwerte sich deshalb ein Petent, der seine aus Anlass einer Bürgerbefragung – vertraulich – geäußerte Meinung auf einer eigens dafür gefertigten Plakatwand in der Öffentlichkeit wiederfand.

Die Gemeinde sprach zwar von einer „Verkettung unglücklicher Umstände“, die zu dem eingeräumten Verstoß geführt habe. Wenn jedoch nur ein Glied in dieser "Kette" sich auf den Datenschutz besonnen hätte, wäre die Äußerung bei der Bürgerbefragung vertraulich geblieben; so war es auch auf den schriftlichen Fragebögen - den gesetzlichen Bestimmungen entsprechend – zugesichert gewesen. Stattdessen wurde die Meinungsäußerung des Petenten in öffentlicher Sitzung des Ortsrates sogar verlesen, die Prangerwirkung für den Petenten in der Öffentlichkeit damit erst recht in Gang gesetzt.

Ich habe dies beanstandet und darüber hinaus den Petenten auf sein Recht hingewiesen, Strafantrag wegen Verletzung seiner Persönlichkeitsrechte nach §§ 203, 205 Strafgesetzbuch zu stellen. Ob und inwieweit eine weitere Stelle dafür gesorgt hat, dass die Meinungsäußerung – über die öffentliche Sitzung im Ortsrat hinaus - auch noch auf einer Plakatwand verbreitet wurde, konnte ich nicht klären; für die nicht-öffentliche Stelle war meine Kontrollkompetenz nicht gegeben. Aufgrund der Ermittlungsbefugnis der Staats-

anwaltschaft können jedoch beide Sachverhaltskomplexe erfasst werden, sofern der Petent den erforderlichen Strafantrag gestellt hat.

8.3 Anti-Korruptionsstelle bei einer Kommune

Aus der Presse habe ich entnommen, dass eine Kommune bei ihrem Rechnungsprüfungsamt eine Anti-Korruptionsstelle eingerichtet hat.

Jede öffentliche Stelle muss auf rechtmäßiges Handeln ihrer Mitarbeiter bedacht sein und Vorsorge dafür treffen, dass Unregelmäßigkeiten erkannt und Pflichtverstöße geahndet werden können; das bedingt entsprechende Informationen. Bekanntermaßen ist aber die Datenverarbeitung aus Anlass des Verdachts eines Korruptionsfalles nicht unproblematisch; es wird mit sehr sensiblen Daten umgegangen, da es sich in dem Einzelfall stets um Dienstpflichtverletzungen und auch um Verstöße gegen Straftatbestände handelt.

Zur Grundlage ihrer Handlungsanweisung für den Umgang mit korruptionsgefährdenden Sachverhalten hatte die Kommune einen alten Erlass des Ministeriums des Innern aus dem Jahre 1976 über die Annahme von Belohnungen und Geschenke durch Angehörige des öffentlichen Dienstes gemacht. Gegen die Regelung dieses alten Erlasses, der leider nach wie vor nichts an Aktualität eingebüßt hat, ist aus Datenschutzsicht nichts einzuwenden.

Auch die Ansiedlung der Anti-Korruptionsstelle beim Rechnungsprüfungsamt, die auf den ersten Blick bedenklich erscheinen mag, konnte auch aus der Sicht des Datenschutzes durchaus als sachgerecht angesehen werden. Hauptaufgabe der Anti-Korruptionsstelle ist es, Sachverhalte aufzuklären, um gegenüber der Staatsanwaltschaft und in Disziplinarverfahren als kompetente Ansprechpartnerin für diese Stellen tätig werden zu können. Dies lässt sich mit der Aufgabe des Rechnungsprüfungsamtes meines Erachtens vereinbaren, da auch dort, wenn auch zu Zwecken der Rechnungsüberprüfung, ein umfassendes Akteneinsichts- und Auskunftsrecht besteht, das auch die Bekanntgabe personenbezogener Daten beinhalten kann. Dies wurde für die Anti-Korruptionsstelle in der Dienstanweisung nochmals bekräftigt, wenn auch die beiden Aufgabenbereiche strikt voneinander zu trennen sind.

Zu einem Punkt der Dienstanweisung habe ich jedoch um eine Modifizierung des Wortlautes gebeten. Allen Mitarbeiterinnen und Mitarbeitern sollte es zur Dienstpflicht gemacht werden, nicht nur festgestellte, sondern auch „vermutete“ Korruptionsfälle unverzüglich der Anti-Korruptionsstelle mitzuteilen. Es kann nach meiner Ansicht schwerlich zum Inhalt einer Dienstpflicht von Bediensteten gemacht werden, Vermutungen zu äußern. Damit würde der Einzelne auch aufgefordert, sich weit in das Vorfeld eines Straf-

tatenverdachts zu begeben und aus dieser Warte heraus, Daten über andere Personen zu übermitteln.

Ich habe vorgeschlagen, erst dann eine Dienstpflicht zu statuieren, wenn tatsächliche Anhaltspunkte einen Verdacht untermauern. Die Kommune hat zugesagt, meinem Vorschlag zu folgen und die Dienstanweisung in diesem Punkt umzuformulieren.

9 Ausländer

9.1 Privatisierung der Abschiebehaft

In einigen Bundesländern wird die Privatisierung oder Teilprivatisierung des Strafvollzugs und auch des Maßregelvollzugs in Erwägung gezogen oder bereits praktiziert.

Im Saarland wurde zeitweilig ein privater Sicherheitsdienst zum Vollzug der Abschiebehaft eingesetzt. Von diesem Vorhaben wurde ich leider erst durch einen Kollegen in Kenntnis gesetzt, obwohl es sich hier um einen Fall der Auftragsdatenverarbeitung handelt, über die ich nach dem Datenschutzgesetz zu unterrichten gewesen wäre.

Die Probleme, die sich in diesem Zusammenhang stellen, wurden daraufhin mit der Leitung der betreffenden Vollzugsanstalt und dem für das Ausländerrecht zuständigen Innenministerium erörtert.

Von Seiten der Vertreter der Justizvollzugsanstalt wurde betont, dass es dem privaten Sicherheitsdienst nicht erlaubt sei, eigenständige Tätigkeiten auszuüben; ein Hoheitsträger (Justizvollzugsbediensteter) sei stets verfügbar, um gegebenenfalls eingreifen, insbesondere auch unmittelbaren Zwang ausüben zu können. Dies sei dem privaten Sicherheitsdienst verwehrt. Er handle folglich als unselbständiger Verwaltungshelfer bzw. Erfüllungsgehilfe. Eine Dienstanweisung mit eingehenden weiteren Hinweisen legte die Tätigkeiten und Pflichten im Einzelnen fest.

Die darstellte Handhabung habe ich in Übereinstimmung mit den (wenigen) einschlägigen Bestimmungen des Strafvollzugsgesetzes zur Abschiebehaft als sogenannte Sicherungshaft gesehen.

Dagegen habe ich als Beispiel für eine nicht privatisierbare Tätigkeit die Haftraumkontrolle genannt. Diese war in der Vergangenheit bereits durch die Verfügung eines Leiters einer Justizvollzugsanstalt als hoheitliche Maßnahme bezeichnet worden, die nur von staatlichen Bediensteten durchgeführt werden dürfe. Der Vertrag mit der beauftragten Sicherheitsfirma enthielt demgegenüber ausdrücklich unter anderem auch die Aufgabe der Haftraumkontrolle. Für diese Tätigkeit war daher besonders zu unterstreichen,

dass das Unternehmen nicht anstelle des Hoheitsträgers selbständig handeln darf.

Nicht zuletzt war bei der Prüfung noch zu betonen, dass die ohnehin zu langen Aufbewahrungsfristen für die Unterlagen der Strafvollzugshäftlinge nicht auf die Abschiebehaft übertragen werden dürfen. Die Möglichkeit einer erneuten Haft in Deutschland nach erfolgter Abschiebung halte ich für einen äußerst seltenen Ausnahmefall, so dass kurze Aufbewahrungsfristen für solche Unterlagen festzulegen wären.

Die mit der Justizvollzugsanstalt und dem Ministerium erörterten Probleme werden im Jahre 2001, wie durch das Ministerium angekündigt wurde, im Saarland nicht mehr weiterbestehen, da die hier angeordnete Abschiebehaft in einem anderen Bundesland vollzogen wird.

9.2 Auskunfts- bzw. Löschungsersuchen zu im Schengener Informationssystem (SIS gespeicherten Daten)

Sogenannte Drittausländer nach dem Durchführungsübereinkommen zwischen den Regierungen der Schengen-Vertragsstaaten machen nach einer Ausweisung, Zurückweisung oder Abschiebung aus der Bundesrepublik Deutschland zunehmend öfter Gebrauch von ihrem Auskunftsrecht nach Art. 109 des Schengener Durchführungsübereinkommens. Ein Drittausländer ist nach der Definition dieses Übereinkommens jede Person, die nicht Staatsangehöriger eines der Mitgliedsstaaten der Europäischen Gemeinschaften ist. Die Ersuchen auf Auskunft und Löschung erreichen die Landesbeauftragten für Datenschutz über den Bundesbeauftragten, dem die Schreiben in der Regel durch die ausländischen Datenschutzinstanzen des Landes zugeleitet werden, in dem der Ausländer sich aufhält.

Den Ausländern geht es meist neben der Auskunft um die Korrektur unrichtiger Ausschreibungen, aufgrund derer sie an der (erneuten) Einreise gehindert werden. Häufig ist die Frage, nach welcher Frist der Drittausländer wieder in die Bundesrepublik Deutschland oder in den Schengen-Vertragsraum einreisen darf, für den Auskunftsbegehrenden von existenzieller Bedeutung. Bei der Kontrolle der Ausschreibungen haben wir daher diesem Aspekt besondere Beachtung geschenkt.

Von Bedeutung sind die im Schengener Informationssystem zur Einreiseverweigerung aufgeführten Fristen sowie die nationalen Fristen in den Fahndungshilfsmitteln der Polizei, in denen der Ausländer parallel ausgeschrieben werden darf. Auch für die Eingabe in die nationale Fahndungsdatei der Polizei ist von der Ausländerbehörde das Fristende nach dem Ausländerrecht vorzugeben und darf, sofern nicht polizei- oder strafrechtliche Gründe den Fristablauf mit beeinflussen, nicht vom zufälligen Zeitpunkt abhängen, zu dem die Polizei die Ausschreibung bearbeitet. Die Polizei

handelt insofern im Rahmen einer Auftragsdatenverarbeitung für die Ausländerbehörde, die als Auftraggeberin die Verantwortung für die Datenverarbeitung trägt (§ 5 SDSG).

Bei einer stichprobenartigen Überprüfung von ausgeschriebenen Fällen im Landesamt für Ausländer- und Flüchtlingsangelegenheiten, das wohl für die Mehrzahl der Ausschreibungen zuständig ist, stellten wir fest, dass insoweit keine Vorgaben bestanden. Es wurde dann festgelegt, dass korrektes Datum für den Beginn und damit auch maßgebend für das Ende des Fristenlaufs der Tag der Abschiebung ist. Das Landesamt hat nach der Prüfung in einigen Fällen die Fristen korrigiert, so dass letztlich auch Löschungen zu veranlassen waren.

An dieser Stelle sei daran erinnert, dass das Recht auf informationelle Selbstbestimmung allen Menschen, unabhängig von ihrer Staatsangehörigkeit, als Menschenrecht zusteht.

10 Meldewesen

10.1 (Geplante) Änderungen des Melderechts

Das Landesmelderecht ist dem Zweiten Gesetz zur Änderung des Melderechtsrahmengesetzes bis zum 1. August 2001 anzupassen. Ein entsprechender Änderungsentwurf zum Landesmeldegesetz liegt mir bislang noch nicht vor, ich gehe indes davon aus, dass ich noch zeitgerecht beteiligt werde. Wie bereits in meinem 17. TB (TZ 16.1) berichtet, sollte mit den Änderungen zur Vorbereitung einer erneuten, diesmal jedoch registergestützten Volkszählung die Qualität der Melderegister verbessert werden. Dazu ist im Bundesrecht (Sozialgesetzbuch X) schon eine Vorschrift zur Durchbrechung des Sozialgeheimnisses in Kraft getreten, die es erlaubt, die Meldebehörde über die Unrichtigkeit oder Unvollständigkeit von zuvor auf Grund Melderechts übermittelter Daten zu unterrichten.

Ein Drittes Gesetz zur Änderung des Melderechtsrahmengesetzes ist zur Zeit ebenfalls in der Diskussion. Von besonderer Auswirkung wäre die Erwägung, Meldedaten, wenn auch nur im Umfang der einfachen Melderegisterauskunft, im Internet allgemein zugänglich zu veröffentlichen. Die damit verbundenen Gefahren sind nicht wesentlich anders zu beurteilen als bei der Veröffentlichung von Adressbüchern und elektronischen Adressverzeichnissen, wofür im Landesrecht ausdrücklich die Einwilligung des Betroffenen vorgesehen ist. Bei der unmittelbaren Abrufmöglichkeit für jedermann gäbe es keine Möglichkeit, das Interesse des Auskunftsbegehrenden mit etwa entgegenstehenden Interessen des Betroffenen abzuwägen; ein Widerspruch, wie ihn die EG-Datenschutzrichtlinie vorsieht, hätte faktisch keine Chance. Eine solche Änderung wäre abzulehnen.

Dagegen ist aus Sicht des Datenschutzes positiv, dass in Betracht gezogen wird, die Zulässigkeit der Herausgabe von Daten an Parteien und andere Gruppierungen vor Wahlen an die Einwilligung des Betroffenen zu knüpfen (s.a. 17. TB Anlage 19.13).

10.2 Jugendabstimmung zur Trassenführung der Saarbahn

Einen melde- und kommunalrechtlich interessanten Fall hatten wir aufgrund einer Eingabe zu erörtern; es ging um die Frage, ob und welche Daten im Rahmen einer Gruppenauskunft einem Bürgermeister ausgehändigt werden dürfen, der sie nach seinen Angaben jedoch in erster Linie als Privatperson verlangt hat. Anlass hierfür war die in seiner Gemeinde parteipolitisch umstrittene Absicht, zur Trassenführung einer geplanten Nahverkehrsanbindung auch Jugendliche des Ortes zu befragen.

Die Saarbahn soll zukünftig auch zu den umliegenden Gemeinden der Stadt Saarbrücken bis hin ins nördliche Saarland führen. Die betreffende Gemeinde wollte die Meinung der Bevölkerung hierzu feststellen; es gab intern heftige Debatten darüber, welche Bevölkerungsgruppen in die Diskussion über den Trassenverlauf miteinbezogen werden sollten. Nachdem der Gemeinderat eine Ordnung für die Einwohnerbefragung beschlossen hatte, die allein das Befragen der Erwachsenen vorsah, hatte der Bürgermeister das Meldeamt um eine Gruppenauskunft gebeten, um seinerseits als "Privatperson" eine Befragung der Jugendlichen durchführen zu können.

Die Adressdaten aller Jugendlichen der Gemeinde wurden ihm zu diesem Zweck übermittelt. Nach der Ablehnung im Gemeinderat war kein Wunder, dass bei der Durchführung Beschwerden laut wurden, weil sowohl eine Beeinflussung des Ergebnisses der Jugendbefragung durch die jeweilige Elternmeinung befürchtet als auch umgekehrt unangebrachter Druck auf die offizielle Einwohnerbefragung mit der Jugendabstimmung angenommen wurde. Nach dieser Auffassung konnte die Absicht, die Jugendlichen zu befragen, dem Gemeinderatsbeschluss zuwiderlaufen. Ausdrücklich wurde auch die datenschutzrechtliche Zulässigkeit bezweifelt; denn wenn wegen der vom Gemeinderat festgelegten Befragung allein der Erwachsenen eine Jugendabstimmung gar nicht hätte stattfinden dürfen, wäre eine weitere Datenübermittlung nicht mehr erforderlich gewesen.

Nach meinem Eindruck spielte zwar der Datenschutz in der politischen Auseinandersetzung eine durchaus nachrangige Rolle. Von Bedeutung war jedoch aus Sicht des Datenschutzes, ob auch jede andere Privatperson auf der Grundlage der melderechtlichen Auskunftsnorm eine Gruppenauskunft erhalten hätte, die nach Melderecht ein "öffentliches Interesse" voraussetzt. In diesem Zusammenhang stellte sich die Frage, ob der Gemeinderatsbeschluss eben dieses bei dem vorliegenden Thema nicht schon allgemein verbindlich festgelegt hatte. Zudem hatte der Bürgermeister bei dem als Pri-

vatperson gestellten Antrag auf das Interesse hingewiesen, das er als Amtsperson an dem Ergebnis der geplanten Jugendabstimmung habe.

In Übereinstimmung mit einer renommierten Literaturmeinung hat das mit dem Fall ebenfalls befasste Innenministerium dargelegt, unter "öffentlichem Interesse" sei auch jedes soziologisch-gesellschaftliche Interesse zu verstehen, so dass eine Gruppenauskunft an eine Privatperson zulässig gewesen sei. Es hat gegen das Handeln der örtlichen Meldebehörde keine Einwände erhoben.

Diese Auffassung halte ich nur dann für zutreffend, wenn man den Gemeinderatsbeschluss und die Datenübermittlung aus dem Melderegister isoliert betrachtet. Leider hat das Innenministerium nicht dazu Stellung genommen, ob das öffentliche Interesse nicht schon bereits durch den Gemeinderatsbeschluss abgedeckt war, so dass weitere Übermittlungen nicht mehr erforderlich gewesen wären. Aber selbst dann war festzuhalten, dass eine ebenfalls ermessensgerechte, aber datenschutzfreundlichere Entscheidung der Meldebehörde zu einer Auskunftsverweigerung hätte führen können. Es ließ sich keinesfalls mit Sicherheit für die Gruppenauskunft ausschließen, dass die amtliche Funktion des Bürgermeisters in der Waagschale der Ermessensentscheidung zugunsten der Datenübermittlung an eine Privatperson den Ausschlag gegeben hatte.

Ich halte es auch nicht für generell vertretbar, jeder Einzelperson, die sich eines soziologisch-gesellschaftlichen Themas außerhalb der zuständigen Gremien und Behörden annimmt, eine Gruppenauskunft zu erteilen, die zudem in diesem Einzelfall die beträchtlich große Gruppe aller Jugendlichen der Gemeinde umfasste.

10.3 Anfrage der Steuerfahndung zum Aufenthalt eines Bürgers in der Psychiatrischen Abteilung eines Krankenhauses

Weil dort mit ganz besonders sensiblen Daten umgegangen wird, lag nahe, dass in der psychiatrischen Abteilung eines Krankenhauses die Zulässigkeit einer Anfrage bezweifelt wurde, mit der die Steuerfahndung die Anwesenheit eines Patienten bestätigt haben wollte. Auf Anfrage der Klinik führte hingegen die Prüfung der Rechtslage zu einem eindeutigen – positiven - Ergebnis.

Nach Melderecht haben die in Krankenhäusern aufgenommenen Personen dem Leiter des Krankenhauses oder seinem Beauftragten die erforderlichen Angaben über ihre Identität zu machen. Das Krankenhaus ist verpflichtet, diese Angaben unverzüglich in ein Verzeichnis aufzunehmen. Der Meldebehörde und der Polizei ist aus dem Verzeichnis Auskunft zu erteilen, wenn dies nach deren Feststellung zur Abwehr einer erheblichen und gegenwärti-

gen Gefahr, zur Verfolgung von Straftaten oder zur Aufklärung des Schicksals von Vermissten und Unfallopfern im Einzelfall erforderlich ist.

Zusätzlich war darauf hinzuweisen, dass die Finanzbehörde im Steuerstrafverfahren nach der Abgabenordnung die Rechte und Pflichten wahrnimmt, die der Staatsanwaltschaft in Ermittlungsverfahren zusteht. Für die eingesetzten Beamten sind die für Hilfsbeamte der Staatsanwaltschaft geltenden Vorschriften der Strafprozessordnung entsprechend anwendbar, so dass die Beamten der Steuerfahndung im vorliegenden Fall Polizeibeamten gleichzustellen sind.

Zur Verfolgung von Steuerstraftaten konnte die Steuerfahndung daher zu Recht Auskunft aus dem vom Krankenhaus zu führenden Verzeichnis verlangen. Die korrespondierende bereichsspezifische Bestimmung im Krankenhausgesetz führte zu demselben Ergebnis, denn danach ist die Übermittlung zulässig, wenn eine Rechtsvorschrift, hier das Melderecht, dies erlaubt.

11 Soziales

11.1 Auskunft über bei der Krankenkasse gespeicherte Daten

Die Versicherte einer gesetzlichen Krankenkasse wollte von ihrer Krankenkasse wissen, welche Diagnosen dort im Zusammenhang mit einer augenärztlichen Behandlung gespeichert sind.

Die Kasse verweigerte die Auskunft mit der Begründung, es handele sich um besonders schutzwürdige personenbezogene Daten, über die die Krankenkassen prinzipiell auch gegenüber dem Versicherten keine Auskunft erteilen dürften.

Empört wandte sich die Petentin an meine Dienststelle. Als Betroffener müsste ihr doch die begehrte Auskunft erteilt werden.

Die betreffende Petentin hatte selbstverständlich recht. Im Sozialgesetzbuch (SGB X – Verwaltungsverfahren) ist geregelt, dass dem Betroffenen auf Antrag Auskunft zu erteilen ist über die zu seiner Person gespeicherten Sozialdaten, deren Herkunft und Empfänger sowie den Zweck der Speicherung (§ 83 Abs. 1 Satz 1 SGB X).

Gleichwohl hatte das Auskunftsersuchen nur teilweise Erfolg. Das hängt damit zusammen, dass den Krankenkassen im Rahmen der Abrechnung ärztlicher Leistungen von niedergelassenen Ärzten keine auf den einzelnen Versicherten bezogenen Diagnosedaten mitgeteilt werden.

Aufgrund meiner Intervention hat die betreffende Krankenkasse aber alle Daten mitgeteilt, die bei ihr über die Petentin gespeichert waren.

11.2 Bestellung eines Datenschutzbeauftragten

Die Sozialversicherungsträger, also z.B. die Krankenkassen, die Berufsgenossenschaften oder die Rentenversicherungsträger, sind verpflichtet, einen Datenschutzbeauftragten zu bestellen (§ 81 Abs. 4 SGB X). An diesen Datenschutzbeauftragten stellt das Gesetz bestimmte Anforderungen, wie Fachkunde und Zuverlässigkeit (§ 36 Abs. 2 BDSG). Dabei ist Zuverlässigkeit nicht nur im Sinne einer charakterlichen Anforderung für die Aufgabenerfüllung zu verstehen. Die Gefahr einer nicht ordnungsgemäßen Aufgabenerfüllung besteht ebenso, wenn der Datenschutzbeauftragte neben dieser Tätigkeit noch andere Funktionen wahrnimmt, die zu Interessenkonflikten führen können.

Eine solche Situation habe ich bei einem meiner Kontrolle unterliegenden Sozialversicherungsträger gesehen, der den Personalleiter mit der Funktion des Datenschutzbeauftragten betraut hatte. Im Personalbereich werden in erheblichem Umfange personenbezogene Daten sensibler Art verarbeitet. Jemand, der Personalentscheidungen trifft oder vorbereitet und für die Verarbeitung der Personaldaten zuständig und verantwortlich ist, darf nicht gleichzeitig die datenschutzrechtliche Kontrolle über diese Datenverarbeitung ausüben.

Erst nachdem ich die Bestellung des Personalleiters zum Datenschutzbeauftragten förmlich beanstandet habe, hat sich der betreffende Sozialversicherungsträger bereit erklärt, den Leiter der Abteilung Innenrevision zum Datenschutzbeauftragten zu bestellen.

11.3 Anfrage beim Arbeitgeber im Rahmen der Sozialhilfe

Für die Gewährung von Sozialhilfe sind die Einkommens- und Vermögensverhältnisse des Antragstellers von grundlegender Bedeutung. Die Petentin im vorliegenden Fall wurde deshalb vom Sozialamt aufgefordert, ihre Einkommensverhältnisse darzulegen und eine Verdienstbescheinigung ihres Arbeitgebers vorzulegen. Dieser Aufforderung kam die Petentin nach, indem sie ein Schreiben ihres Arbeitgebers vorlegte, in dem der Beginn ihrer Beschäftigung, die monatliche Arbeitszeit und der Verdienst pro Stunde bescheinigt wurden.

Diese Bescheinigung entsprach jedoch nicht den Vorstellungen des zuständigen Sachbearbeiters beim Sozialamt von einer ordnungsgemäßen Verdienstbescheinigung. Unter dem Briefkopf „Sozialamt“ schrieb er den Ar-

beitgeber der Petentin an und bat um Ausfüllung eines amtlichen Formulars mit den nach seiner Ansicht erforderlichen Angaben.

Die Petentin beschwerte sich bei meiner Dienststelle darüber, dass auf diese Weise ihrem Arbeitgeber ohne Not bekannt gegeben worden sei, dass sie Sozialhilfeempfängerin sei.

Auch nach meiner Auffassung entsprach die Vorgehensweise des Sozialamtes im vorliegenden Fall nicht den datenschutzrechtlichen Bestimmungen. Zwar ist der Arbeitgeber gemäß § 116 Abs. 2 Bundessozialhilfegesetz verpflichtet, dem Träger der Sozialhilfe über die Art und Dauer der Beschäftigung, die Arbeitsstätte und den Arbeitsverdienst des Hilfesuchenden Auskunft zu geben. Allerdings muss das Sozialamt gemäß § 67a SGB X zunächst versuchen, die Daten beim Betroffenen selbst zu erheben. Davon ist es im vorliegenden Fall offensichtlich auch ausgegangen, indem es die Petentin zunächst aufgefordert hatte, selbst eine Verdienstbescheinigung vorzulegen. Die Problematik im vorliegenden Fall lag darin, dass man der Petentin von Seiten des Sozialamtes nicht eindeutig gesagt hatte, welchen Inhalt eine ordnungsgemäße Verdienstbescheinigung haben muss. Die Verantwortung, dass es hier zu einer überflüssigen Offenbarung des Sozialhilfebezugs gegenüber dem Arbeitgeber der Petentin gekommen ist, lag somit eindeutig beim Sozialamt.

Damit sich dieser Fall in Zukunft bei anderen Antragstellern nicht wiederholt, muss das Sozialamt den Antragstellern eindeutig sagen, welche Unterlagen mit welchem Inhalt vorzulegen sind.

11.4 Ermittlungen des Sozialamtes bei Nachbarn

Ein Petent wollte wissen, ob sich das Sozialamt in folgendem Fall datenschutzrechtlich korrekt verhalten hatte:

Da das Sozialamt wegen verschiedener tatsächlicher Anhaltspunkte eine eheähnliche Gemeinschaft mit seiner Freundin vermutete, wurden Ermittlungen bei dem Vermieter und einer Nachbarin des Petenten vorgenommen. Der Petent war der Auffassung, das Sozialamt habe nicht das Recht, Nachforschungen in seinem Privatleben anzustellen.

In dieser Allgemeinheit und im konkreten Fall konnte ich dem Petenten nicht zustimmen. Denn gemäß § 20 SGB X hat die Sozialbehörde den Sachverhalt von Amts wegen zu ermitteln. Sie bestimmt Art und Umfang der Ermittlungen und hat alle für den Einzelfall bedeutsamen Umstände zu berücksichtigen. Die Behörde bedient sich der Beweismittel, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich hält; sie kann insbesondere Auskünfte jeder Art einholen, Beteiligte anhören,

Zeugen und Sachverständige vernehmen und den Augenschein einnehmen (§ 21 Abs. 1 SGB X).

Auch die Vorschrift des § 67a Abs. 2 Satz 1 Nr. 2 SGB X führt zu keiner anderen Beurteilung. Sie formuliert die Einschränkung des generellen datenschutzrechtlichen Prinzips, dass Erhebungen vorrangig bei dem Betroffenen selbst zu erheben sind. Nach dieser Vorschrift können aber Sozialdaten bei dritten Personen unter anderem erhoben werden, wenn die Aufgaben ihrer Art nach eine Erhebung bei anderen Personen erforderlich machen und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

Das Sozialamt hat überzeugend dargelegt, dass Anhaltspunkte für das Bestehen einer eheähnlichen Gemeinschaft vorlagen. Die Befragung der Zeugen waren geeignete und erforderliche Maßnahmen zur weiteren Sachverhaltsaufklärung. Auch waren keine überwiegenden schutzwürdigen Interessen des Petenten erkennbar, die eine Befragung dritter Personen ausgeschlossen hätten.

Es ist also keineswegs so, dass der Datenschutz von vornherein Ermittlungen der Sozialbehörden unmöglich macht. Entscheidend ist, dass sich die Ermittlungen im Rahmen der gesetzlichen Befugnisse bewegen.

11.5 Beschlagnahme von Jugendhilfeakten

Ein Jugendamt hat mich um meine Rechtsauffassung zu folgender Fallkonstellation gebeten:

Ein Amtsgericht hatte die Beschlagnahme von Akten des betreffenden Jugendamtes angeordnet. Gegen diesen Beschluss hatte das Jugendamt Beschwerde mit der Begründung eingelegt, die eingesehene Akte enthalte Sozialdaten, die einem Mitarbeiter des Jugendamtes zum Zwecke persönlicher und erzieherischer Hilfe anvertraut worden seien (§ 65 SGB VIII). Das zuständige Landgericht hat die Beschwerde als unbegründet verworfen.

Die rechtsprechende Tätigkeit der Gerichte unterliegt zwar nicht meiner Datenschutzkontrolle; ich konnte den konkreten Fall also nicht bewerten. Gleichwohl habe ich mich mit der Problematik befasst, um dem betreffenden Jugendamt Hilfen für ihr Verhalten in vergleichbaren künftigen Fällen zu geben.

Zunächst stellt sich meiner Auffassung nach das Verhältnis der Prozessordnungen, die eine Auskunftspflicht und eine Vorlagepflicht von Akten und Unterlagen regeln, zu den Vorschriften über den Sozialdatenschutz so dar, dass bei Anforderung von Sozialdaten die Schranken des Sozialdatenschutzes zu prüfen sind. Dies ergibt sich aus § 35 Abs. 3 SGB I, wonach keine Auskunftspflicht, keine Zeugnispflicht und keine Pflicht zur Vorlegung oder

Auslieferung von Schriftstücken, Akten und Dateien besteht, soweit eine Übermittlung von Sozialdaten nicht zulässig ist. § 35 beschränkt insoweit die Bestimmungen in Prozessordnungen, denen zufolge das Gericht die Vorlage von Unterlagen verlangen kann.

Es muss deshalb geprüft werden, ob die Datenübermittlung nach den sozialdatenschutzrechtlichen Vorschriften zulässig ist. Im Bereich der Jugendhilfe ist insbesondere die einschränkende Normierung in § 65 SGB VIII zu beachten, wonach Sozialdaten, die dem Mitarbeiter eines Trägers der öffentlichen Jugendhilfe zum Zweck persönlicher und erzieherischer Hilfe anvertraut worden sind, nur unter bestimmten Voraussetzungen offenbart werden dürfen. Bei der Beratung anvertraute Daten dürfen nur mit Einwilligung offenbart werden, darüber hinaus unter bestimmten Voraussetzungen gegenüber dem Vormundschafts- oder dem Familiengericht sowie unter den Voraussetzungen, unter denen eine Strafbarkeit nach § 203 Strafgesetzbuch ausscheiden würde. Letzteres betrifft vor allem den Fall des Notstandes gemäß § 34 Strafgesetzbuch, also eine Abwägung zwischen den Rechtsgütern bei begangenen schweren Straftaten.

Der Gesetzgeber hat sich ganz bewusst für einen besonderen Schutz von Daten entschieden, die ein Betroffener freiwillig in einer Beratungssituation den Mitarbeitern des Jugendamtes anvertraut.

11.6 Unzulässiger Datenabgleich zwischen Stadtwerken und Sozialamt

Durch eine Eingabe habe ich erfahren, dass das Energieunternehmen einer Stadt Guthaben bei der Jahresverbrauchsabrechnung nicht wie üblich den Kunden auszahlte, sondern zunächst das städtische Sozialamt informierte. Das Sozialamt stellte anhand der Liste fest, welche Personen Sozialhilfe erhielten, und veranlasste bei den Stadtwerken, dass dem Sozialamt zustehende Teilbeträge der Guthaben (z. B. Fernwärmekosten) kurzerhand verrechnet wurden.

Die gutgemeinte Absicht, finanzielle Ansprüche der Stadt zu sichern, rechtfertigt nicht jedes Mittel. Durch Mitwirkung der Hilfeempfänger (etwa Anfordern der Verbrauchsabrechnung bei den infrage kommenden Leistungsempfängern) könnte dieser Zweck auch ohne Datenabgleich erreicht werden, ohne über die Köpfe der Betroffenen hinweg zu handeln und ohne die Auszahlung der Guthaben unbeteiligter Kunden zurückzuhalten. Die Stadt hatte in einer ersten Stellungnahme zu erkennen gegeben, dass sie an dem Datenabgleich festhalten wolle. Erst nachdem ich die mit diesem Verfahren verbundenen Datenübermittlungen formell als unzulässig beanstandete, weil sie ohne Rechtsgrundlage erfolgten, hat mir der Oberbürgermeister mitgeteilt, dass der Datenabgleich eingestellt wird.

11.7 Beitragsfreistellung in Kindergärten

Durch Änderung des Vorschulgesetzes werden die Erziehungsberechtigten der Kinder im letzten Kindergartenjahr ab August 2000 von der Zahlung des Elternbeitrages freigestellt. Für die Erstattung des Beitragsausfalls sollten die Kindergärten dem Ministerium für Bildung, Kultur und Wissenschaft eine Liste der betroffenen Kinder mit Angabe der Namen, Vornamen, Geburtsdaten und Wohnort vorlegen.

Für die Leistungsgewährung durch das Ministerium kommt es nur auf die Höhe der Ausfälle an; hierfür benötigt es nicht die genaue Kenntnis der personenbezogenen Daten. Die Datenerhebung sollte nur der Kontrolle der ordnungsgemäßen Abrechnung durch die Einrichtungen dienen; dieser Zweck kann auch dadurch erreicht werden, dass die Übermittlung auf solche Daten beschränkt wird, die den Personenbezug nicht unmittelbar deutlich werden lassen. Ich habe vorgeschlagen, in der dem Ministerium vorzulegenden Liste den Namen wegzulassen. Die Einrichtungen sollten die gleiche Liste mit allen Daten vorhalten, um das Ministerium in die Lage zu versetzen, stichprobenweise eine Kontrolle der Richtigkeit der Angaben vorzunehmen.

Das Ministerium hat meine Vorschläge in sein Rundschreiben an die Kindergartenträger eingearbeitet.

11.8 Liste sozialer Brennpunkte

Ein städtisches Sozialamt hatte eine Liste von Großwohnanlagen und sozialen Brennpunkten mit Adressen sowie Namen und Telefonnummern der Hausverwalter und Hausmeister zusammengestellt und wollte diese Liste anderen Stadtämtern und externen Stellen wie Polizei, Feuerwehr, Kreisjugendamt, Gesundheitsamt, Rettungswache zur Verfügung stellen. Die Liste enthielt personenbezogene Daten der Hausmeister und -verwalter; ohne deren Einwilligung oder ohne konkreten Anlass sollten die Daten keinesfalls weitergegeben werden.

Unabhängig davon hielt ich die Liste für problematisch. Die Angaben könnten die Sachbearbeiter im Sozialamt veranlassen, Wohn-, Miet- und andere Angelegenheiten der Hilfeempfänger - über den Kopf der Betroffenen hinweg - unmittelbar mit Hausverwalter und Hausmeister zu „regeln“. Hilfesuchende und Hilfeempfänger haben jedoch nicht nur eine Mitwirkungspflicht, sondern auch das Recht, dass Daten unmittelbar bei ihnen selbst erhoben werden. Die Kontaktaufnahme mit Hausverwalter und Hausmeister stellt regelmäßig eine Datenübermittlung dar, deren Zulässigkeit im Einzelfall zu prüfen ist. Mit der Weitergabe der Liste an andere Stellen dokumentiert das Sozialamt, dass in den Wohnanlagen ein hoher Anteil von Sozialhilfeempfängern lebt und dass es sich um „soziale Brennpunkte“ handelt. Damit wer-

den alle Bewohner dieser Häuser - nicht nur die Hilfeempfänger - als sozialschwach abgestempelt.

Das Sozialamt ist meiner Empfehlung gefolgt, zumindest auf die Weitergabe der Liste zu verzichten.

11.9 Datenschutzprüfung beim Landesjugendamt

Das Landesjugendamt ist organisatorisch dem Landesamt für Jugend, Soziales und Versorgung angegliedert, jedoch von diesem räumlich getrennt untergebracht. Es nimmt insbesondere die Aufgaben des überörtlichen Trägers der Jugendhilfe nach dem SGB VIII und der Zentralen Adoptionsvermittlungsstelle wahr.

Die Träger von erlaubnispflichtigen Einrichtungen (z. B. Kinderheime, Kindertagesstätten) sind verpflichtet, Namen und berufliche Ausbildung des Leiters und der Betreuungskräfte bei Betriebsaufnahme und bei Änderungen anzuzeigen. Die vom Landesjugendamt den Einrichtungen vorgegebenen Personalmeldebogen sahen auch die Angabe des Alters der beschäftigten Mitarbeiter vor. Der Gesetzgeber hat in § 47 Abs. 1 Nr. 1 SGB VIII den Umfang der zu meldenden Daten abschließend festgelegt. Das Alter des Personals ist nach dieser Vorschrift nicht zu melden. Das Landesjugendamt sieht künftig von der Erhebung dieser Angabe ab.

Nicht verzichten will das Landesjugendamt dagegen auf die Meldungen der Heime nach § 47 Abs. 2 SGB VIII, die zwar gesetzlich legitimiert sind, deren Notwendigkeit jedoch zu bezweifeln ist. Nach dieser Vorschrift haben die Heime nach jeder Aufnahme eines Kindes dem Landesjugendamt Mitteilung zu geben (lt. Meldebogen mit Name, Staatsangehörigkeit, Geburtstag, Religionszugehörigkeit sowie den Gründen, die zur Heimeinweisung geführt haben, z. B. Vernachlässigung/Misshandlung, sexueller Missbrauch, Erziehungsunfähigkeit der Eltern). Diese Meldungen sind jährlich für alle Kinder zu wiederholen. Zweck der Vorschrift ist, dass die Behörde auf in Heimen „vergessene“ Kinder, die für eine Adoptionsvermittlung infrage kommen, aufmerksam wird. In der Praxis kann die Adoptionsvermittlungsstelle aus diesen Mitteilungen keine Erkenntnisse gewinnen. Der für jedes untergebrachte Kind nach § 36 SGB VIII aufzustellende und regelmäßig zu überprüfende Hilfeplan sollte bereits sicherstellen, dass Kinder nicht länger als erforderlich in Heimpflege bleiben. Abgesehen von dem sensiblen Datenbestand, der unnötigerweise bei der Behörde entsteht, ist auch der den Heimen durch diese Meldepflicht verursachte Aufwand nicht zu unterschätzen. Einige Heime haben dies offensichtlich erkannt und kommen - ohne dass dies zu Sanktionen führt - ihrer Meldepflicht nicht mehr nach. Das Landesjugendamt weist zwar darauf hin, dass das zu erwartende neue Adoptions-

recht diese Mitteilungen voraussichtlich nicht mehr vorsieht. Es will dennoch von sich aus nicht schon jetzt davon absehen, sie zu verlangen.

Zur Verbesserung des Schutzes der Sozialdaten und der Adoptionsdaten habe ich technische und organisatorische Maßnahmen vorgeschlagen:

PC, mit denen sehr sensible Daten verarbeitet werden; z.B. über Adoptionsbewerber, durchgeführte Adoptionen mit detaillierten Angaben über die Adoptiveltern und Adoptivkinder, verfügten über keinerlei Sicherheitsmaßnahmen. Unbefugte konnten ohne weiteres Geräte einschalten, Daten einsehen, verändern, löschen oder auf Diskette kopieren, ohne durch irgendwelche Vorkehrungen, z.B. Eingabe eines Passwortes, daran gehindert zu werden. Ein Sicherheitskonzept für den PC-Einsatz ist zu entwickeln; kurzfristig musste eine Sicherheitssoftware eingesetzt werden.

Das Faxgerät war in einem für alle Mitarbeiter zugänglichen, aber nicht ständig besetzten Raum aufgestellt. Beim Eingang einer Faxmitteilung konnte jeder zufällig dort Anwesende das Fax einsehen; so ist zum Zeitpunkt der Prüfung ein umfangreicher Bericht mit Foto in einer Adoptionssache eingegangen. Das Gerät wurde inzwischen in einen verschließbaren Raum gebracht.

Postausgänge wurden auf einem Tisch im Flur zum Abholen durch den Kurier abgelegt. Die Umschläge waren zwar verschlossen, jedoch konnte jeder Mitarbeiter und Besucher den Adressaten (evtl. ein Adoptionsbewerber) lesen oder Briefe an sich nehmen. Inzwischen wird die Post in einem Büroraum unter Aufsicht zwischengelagert.

Innerhalb des Archivraums sollten zumindest die Adoptionsvermittlungsvorgänge in einem verschlossenen Schrank aufbewahrt werden, der nur den Mitarbeitern der Vermittlungsstelle zugänglich ist.

11.10 Unterhaltssicherung

Unterhaltssicherung wird Wehrpflichtigen und ihren Angehörigen bei der Ableistung von Wehrdienst oder Wehrübungen gewährt. Ich hatte zu prüfen, ob in bestimmten Fallkonstellationen Datenübermittlungen der Unterhaltssicherungsbehörde zulässig sind.

Selbständigen, die zum Wehrpflicht eingezogen werden, kann aus Mitteln der Unterhaltssicherung eine Ersatzkraft zur Fortführung des Betriebs finanziert werden. Da in einem Einzelfall ein Wehrpflichtiger die gewährte Leistung nicht zur Vergütung der Ersatzkraft verwendete, war beabsichtigt, generell der Ersatzkraft eine Kopie des Leistungsbescheids zuzustellen. Offensichtlich erhoffte die Behörde, dass die Ersatzkraft, wenn ihre Vergütung ausbleibt, den Leistungsträger informiert, damit dann die weitere Zahlung eingestellt werden kann. Ich habe dies nicht als geeignetes Mittel angese-

hen, einen Leistungsmissbrauch zu verhindern; die Ersatzkraft ist nämlich in keiner Weise zur Mitteilung an die Behörde verpflichtet. Für die mit der Übersendung der Bescheidkopie verbundene Datenübermittlung an einen privaten Dritten gibt es keine Rechtsgrundlage; sie ist daher unzulässig. Meines Erachtens kann eine zweckentsprechende Verwendung der Leistung besser sichergestellt werden, wenn die Auszahlung der Unterhaltssicherung davon abhängig gemacht wird, dass der Antragsteller Belege über die tatsächliche Vergütung der Ersatzkraft vorlegt. Meinem Vorschlag wurde Rechnung getragen: künftig werden von dem Leistungsempfänger Verwendungsnachweise gefordert.

Außerdem hatte ich zu dem Vorhaben Stellung genommen, den Truppenteilen stets die Höhe der für Selbständige gewährten Unterhaltssicherung mitzuteilen. Dadurch sollte bei der Truppe das Kostenbewusstsein geschärft werden, damit bei künftigen Wehrübungen des betreffenden Reservisten die Notwendigkeit der Einberufung auch unter dem Gesichtspunkt der Kosten- und Leistungsverantwortung kritisch geprüft wird. Auch in diesem Falle habe ich die Datenübermittlung als unzulässig angesehen, weil sie keine geeignete Maßnahme darstellt. Zwar können bei der Heranziehung zu einer Wehrübung u. U. auch finanzielle Erwägungen eine Rolle spielen. Für die Prognose, welche Aufwendungen durch eine anstehende Einberufung anfallen, dürfte allerdings die Kenntnis der früher gewährten Unterhaltssicherung nicht entscheidend sein, da sich sowohl die Tatsache der Selbständigkeit als auch die Höhe des zu berücksichtigenden Einkommens zwischen zwei Wehrübungen ändern kann. Wohl deshalb enthält § 24 Wehrpflichtgesetz, der die Mitteilungspflichten der der Wehrüberwachung unterliegenden Wehrpflichtigen regelt, keine entsprechende Meldepflicht.

11.11 Heimaufsicht

Ich hatte mich in einem Fall mit datenschutzrechtlichen Problemen bei der Heimaufsicht zu beschäftigen, die vom Ministerium für Frauen, Arbeit, Gesundheit und Soziales wahrgenommen wird.

Ein Petent hatte sich darüber beschwert, dass Mitarbeiter der Heimaufsicht sich Zugang zu seinem Anwesen verschafft, dort die Zimmer der Bewohner ohne deren Zustimmung betreten und Einsicht in die Pflegedokumentationen dieser Personen genommen hätten. Dies alles, obwohl er kein Heim betreibe, sondern eine Anlage für sogenanntes "betreutes Wohnen".

Das Betreten der Räume mit Befragen der Bewohner und die Einsichtnahme in Unterlagen mit personenbezogenen Daten stellt eine Datenerhebung dar, die einer gesetzlichen Grundlage bedarf. Die Befugnisse der Heimaufsichtsbehörde sind im Heimgesetz geregelt. Nach § 9 Abs. 2 dieses Gesetzes sind die Mitarbeiter der Heimaufsicht befugt, die für das Heim benutzten Grundstücke und Räume, soweit diese nicht einem Hausrecht der Bewoh-

ner unterliegen, zu betreten. Außerdem darf nach der gleichen Vorschrift Einsicht in die geschäftlichen Unterlagen des Auskunftspflichtigen genommen werden. Ausgehend von diesen Vorschriften habe ich keine datenschutzrechtlichen Bedenken gegen das Vorgehen der Heimaufsichtsbehörde im konkreten Fall geltend gemacht. Auch wenn strittig ist, ob es sich bei einer Einrichtung um ein Heim im Sinne des Heimgesetzes handelt, stehen der Heimaufsicht die genannten Überwachungsmittel zur Verfügung, wenn Anhaltspunkte für das Vorliegen eines Heimes vorliegen.

Zwischenzeitlich gibt es einen Gesetzentwurf der Bundesregierung zur Novellierung des Heimgesetzes. In diesem Gesetzentwurf sind die Befugnisse der Heimaufsichtsbehörde noch konkreter formuliert worden. Außerdem soll mit diesem Entwurf ein Problem gelöst werden, das nach geltenden Gesetzeslage nicht eindeutig und zufriedenstellend gelöst werden konnte, nämlich der Informationsaustausch über Heimprüfungsergebnisse zwischen Heimaufsicht, Medizinischem Dienst, Pflegekassen oder Sozialhilfeträgern. Hier sieht der Entwurf vor, dass die Beteiligten berechtigt und verpflichtet sind, die für ihre Zusammenarbeit erforderlichen Angaben einschließlich der bei der Überwachung gewonnenen Erkenntnisse untereinander auszutauschen. Personenbezogene Daten dürfen in nicht anonymisierter Form an die Pflegekassen und den Medizinischen Dienst der Krankenversicherung übermittelt werden, soweit dies für Zwecke der Pflegeversicherung erforderlich ist. Personenbezogene Daten sind aber sonst generell vor der Übermittlung zu anonymisieren.

11.12 Gesundheitsreform 2000

Breiten Raum in der politischen Diskussion nahm die Gesundheitsreform ein. Hierzu legte die Bundesregierung den Entwurf eines Gesetzes zur Reform der gesetzlichen Krankenversicherung (Gesundheitsreform 2000) vor. Ziele sollten die Verbesserung von Qualität und Wirtschaftlichkeit im Gesundheitswesen sowie die Sicherung der Beitragssatzstabilität in der gesetzlichen Krankenversicherung sein.

In Bezug auf die Daten der Versicherten waren einschneidende Veränderungen gegenüber dem bisherigen System vorgesehen, die teilweise zu unnötigen Eingriffen in die Persönlichkeitsrechte der Betroffenen geführt hätten:

Neu eingeführte "Datenannahmestellen" sollten die von den Kassenärztlichen Vereinigungen, Apotheken, Krankenhäusern, Hebammen und Entbindungspflegern sowie den Erbringern von Heil- und Hilfsmitteln erstellten Abrechnungsdaten auf sachliche Richtigkeit und Rechtmäßigkeit sowie hinsichtlich der Leistungspflicht der Krankenkassen überprüfen. Damit hätte neben den Krankenkassen eine weitere Stelle die Möglichkeit eines - wenn

auch zeitlich begrenzten - umfassenden Zugriffs auf Versichertendaten gehabt. Ein sachlich zwingender Grund hierfür war nicht zu erkennen.

Bisher ist es so, dass die Kassenärztlichen Vereinigungen den Krankenkassen die Abrechnungen der Vertragsärzte über ärztliche Leistungen nur fallbezogen und nicht versichertenbezogen übermitteln dürfen. Dies verfolgt das wichtige datenschutzrechtliche Anliegen zu verhindern, dass bei den Kassen ein umfassendes Bild hinsichtlich der in Anspruch genommenen Leistungen und der entsprechenden Diagnosen in Bezug auf den einzelnen Versicherten entsteht. Die in der Gesetzesbegründung genannten Gründe für die nunmehr vorgesehene versichertenbezogene Speicherung der Abrechnungsdaten überzeugte nicht.

Ihre Kritik zu diesen und einer Vielzahl weiterer datenschutzrechtlicher Verschlechterungen haben die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom 25.8.1999 zum Ausdruck gebracht (Anlage 5). Der Bundestag hat den Entwurf hierauf dahingehend modifiziert, dass die Abrechnungsdaten bei den Annahmedatenstellen pseudonymisiert werden. Die Krankenkassen hätten dann zwar die Daten erhalten, aber nicht gewusst, um welche Patienten es sich handelt. Leider wurden diese Verbesserungen – auch gegenüber dem derzeitigen Zustand - nicht umgesetzt, weil der Bundesrat ihnen nicht zustimmte.

Es gibt allerdings Hinweise, dass das Bundesministerium der Gesundheit datenschutzrechtliche Regelungsvorhaben, auch zur Pseudonymisierung von Versichertendaten bei Abrechnungen gegenüber den Krankenkassen, wieder aufgreifen will.

12 Gesundheit

12.1 Datenschutzprüfung bei einem Gesundheitsamt

Die bisher staatlichen Gesundheitsämter wurden zum 1.1.1997 kommunalisiert. Die Prüfung bei einem Gesundheitsamt hat gezeigt, dass die neue Zuordnung bei diesem Landkreis als solche keine Beeinträchtigung des Datenschutzes mit sich gebracht hat. Postein- und Postausgang sind so organisiert, dass personenbezogene Gesundheitsdaten regelmäßig der Kreisverwaltung nicht bekannt werden.

Mit dem automatisierten Verfahren PINS werden Daten der Bürger erfasst, die mit dem Gesundheitsamt Kontakt hatten, etwa durch ein beantragtes amtsärztliches Zeugnis oder eine meldepflichtige, übertragbare Erkrankung. Einige Grundfunktionen dieses zunächst nur probeweise und nur in Teilbereichen eingesetzten Systems können zu Konflikten mit den Datenschutzregelungen des am 01.01.1999 in Kraft getretenen Gesetzes über den öffentlichen Gesundheitsdienst (ÖGDG) führen. So wäre es mit § 19 Abs. 2

ÖGDG nicht vereinbar, wenn – was offensichtlich Standardfunktion ist („Kontakthistorie“) – später jeder an das System angeschlossene Mitarbeiter stets erkennen könnte, welche Aktivitäten andere Sachgebiete bei dieser Person unternommen haben. Daten, die dem Gesundheitsamt im Zusammenhang mit einer Beratung oder einer freiwilligen Begutachtung anvertraut wurden, dürfen für andere Zwecke nur unter den in dieser Vorschrift genannten Voraussetzungen verwendet werden. Außerdem sieht das System eine elektronische, langfristige Archivierung der amtsärztlichen Gutachten vor. Nach § 21 Abs. 2 ÖGDG ist allerdings die Speicherung der Gutachten in automatisierter Form nicht zulässig.

HIV-Gefährdete werden durch Sozialarbeiter/Sozialpädagogen ohne Angabe personenbezogener Daten beraten. Der HIV-Test erfolgt anonym unter Verwendung eines Pseudonyms. Um die Vertraulichkeit zu erhöhen, habe ich u.a. vorgeschlagen, den Kreis der Personen, die von dem Testergebnis Kenntnis nehmen können, zu reduzieren, und die Unterlagen nach Ablauf des Kalenderjahres zu vernichten. Außerdem ist in der Beratungsstelle auf die Rufnummernanzeige zu verzichten. Die zugesicherte Anonymität der HIV-Beratung ist nicht gewährleistet, wenn die Telefonnummer des anrufenden Klienten am Display zu erkennen ist (bei ISDN- und den häufig genutzten Mobilfunkanschlüssen). Da die Rufnummernanzeige bei der vorhandenen Anlage softwaremäßig nicht zu unterbinden ist, sollte – auch wenn dies mit Einbussen beim Telefonkomfort verbunden ist - ein Endgerät ohne diese Anzeige eingesetzt werden.

Ein HIV-Test wird auch bei sogen. HWG-Personen (u.a. Prostituierte) durchgeführt. Der Test ist ebenfalls freiwillig, jedoch werden die Blutproben gemeinsam mit denen zur Untersuchung auf Geschlechtskrankheiten personenbezogen dem zuständigen Institut zugeleitet. Das Gesundheitsamt hat meinen Vorschlag aufgegriffen, auch für diesen Personenkreis den HIV-Test künftig nicht mehr personenbezogen, sondern unter einem Pseudonym dem Labor zu übersenden. Der Lues-Test ist nach Aufhebung des Gesetzes zur Bekämpfung der Geschlechtskrankheiten seit Anfang 2001 nicht mehr erforderlich.

Bei der schulärztlichen Untersuchung durch den Jugendärztlichen Dienst sollten die Schüler der 4. und 8. Klasse einen Fragebogen ausfüllen, in dem sie Angaben zu ihren Ernährungsgewohnheiten sowie zum Zigaretten-, Alkohol- und Drogenkonsum machen sollten. Ihren Namen sollten die Schüler auf dem Fragebogen nicht angeben; es wurde ihnen vielmehr gesagt, dass es sich um eine anonyme Befragung handele. Die Schüler übergaben den Fragebogen der die Untersuchung durchführenden Schulärztin. Die praktizierte Verfahrensweise ist datenschutzrechtlich problematisch. Es handelte sich um eine Befragung auf freiwilliger Basis, bei der Anonymität in Aussicht gestellt wird. Tatsächlich erfolgte die Datenerhebung personenbezogen, da der den Fragebogen entgegennehmenden Schulärztin die Identität der be-

treffenden Schüler bekannt war. Der Jugendärztliche Dienst hat meine Empfehlung, die Fragebögen zur Wahrung der Anonymität in einen dafür bestimmten Behälter einwerfen zu lassen und die Eltern in dem Anschreiben auch darüber zu informieren, dass die Kinder zu den genannten Themen befragt werden, umgehend in die Tat umgesetzt.

Beschäftigte des Gesundheitsamtes (Ärzte, Sozialarbeiter, Sozialpädagogen) unterliegen nach § 203 Abs. 1 StGB besonderen Geheimhaltungspflichten. Sie sind nicht berechtigt und verpflichtet, bei ihrer Beratungstätigkeit die dienstlichen Telefonkontakte gegenüber dem Arbeitgeber zu offenbaren (vgl. Urteil BAG vom 13.01.1987, NJW 1987,1509, betr. einen bei einem Landkreis angestellten Psychologen). Die Kreisverwaltung hatte deshalb bereits bei der Einführung der automatisierten Telefondatenerfassung den unter § 203 Abs. 1 StGB fallenden Personenkreis von der Erfassung ausgenommen, indem sie spezielle PIN zur Unterdrückung der Zielnummern zur Verfügung stellte. Allerdings hatte sie bei der Zuordnung des Gesundheitsamtes diese Regelung dort nicht umgesetzt, sodass seit Jahren unzulässige Kontrollmöglichkeiten der Hauptverwaltung bestanden. Aufgrund meiner Intervention werden die Zielrufnummern inzwischen auch bei dem infrage kommenden Personenkreis des Gesundheitsamtes nicht mehr aufgezeichnet.

Überrascht hat mich der Umfang und die Zeitdauer der beim Gesundheitsamt aufbewahrten Unterlagen. Es bestätigt die Erfahrung, dass die Verwaltung sich nur schwer von alten Unterlagen trennen kann und dass aufbewahrt wird, solange Platz vorhanden ist. Öffentliche Stellen sind jedoch gesetzlich verpflichtet, personenbezogene Daten zu löschen und Unterlagen zu vernichten, wenn ihre Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist und ein öffentliches Archiv das Material nicht übernimmt (§ 19 Abs. 3 und 4 SDSG). Es ist insbesondere nicht erforderlich, Vorgänge über psychosoziale Beratungen von Behinderten, Süchtigen und psychisch Kranken mit detaillierten Berichten über die gesundheitlichen, familiären, sozialen Verhältnisse, Anklageschriften nach dem Betäubungsmittelgesetz oder Blutgruppenuntersuchungen für Vaterschaftsanerkennungen über Jahrzehnte aufzubewahren. Ich habe gefordert, für die einzelnen Unterlagenarten - soweit noch nicht geschehen – Aufbewahrungsfristen festzulegen und nach deren Ablauf die Vernichtung oder die Abgabe an ein Archiv vorzunehmen. Das Gesundheitsamt hat eine Lösung zugesagt.

12.2 Meldungen nach dem Infektionsschutzgesetz

Bei bestimmten übertragbaren Krankheiten war bereits bisher u.a. der behandelnde Arzt nach dem Bundesseuchengesetz verpflichtet, eine Erkrankung, einen Krankheitsverdacht, einen Ausscheider von Krankheitserregern usw. dem Gesundheitsamt zu melden. Das zum 01.01.2001 in Kraft getrete-

ne Infektionsschutzgesetz (IfSG) hat das aus dem Jahre 1961 stammende Bundesseuchengesetz abgelöst und dabei den Meldekatalog nicht nur den heutigen Gegebenheiten angepasst, sondern auch wesentlich erweitert. Dadurch wurden neue Vordrucke für Ärzte, Labors und Gemeinschaftseinrichtungen notwendig, die ich auf Wunsch des Ministeriums für Frauen, Arbeit, Gesundheit und Sozialordnung aus datenschutzrechtlicher Sicht überprüft habe.

Unterschiedlicher Auffassung waren wir bei der Ausgestaltung der Meldepflicht von Gemeinschaftseinrichtungen wie Schulen, Heime und Kindergärten, die der Gesetzgeber in dieser Form neu eingeführt hat (§ 34 IfSG). Wenn auch das IfSG die Rechtsgrundlage für eine personenbezogene Meldung bietet, stellt sich doch die Frage, ob es erforderlich ist, die Einrichtung zu verpflichten, jede Erkrankung und jeden Krankheitsverdacht von Keuchhusten, Mumps, Windpocken und jede Verlausung von vornherein mit Name und Adresse des Kindes dem Gesundheitsamt zu melden. Ich hätte es vorgezogen, wenn das Gesundheitsamt zunächst nur über den Krankheitsfall - ohne Namen – informiert würde, weil wohl oft keine Notwendigkeit zu konkreten Eingriffen besteht, jedenfalls nicht unmittelbar gegenüber den Einzelpersonen, sondern gegenüber der Einrichtung. Sähe das Gesundheitsamt eine Notwendigkeit, im Einzelfall tätig zu werden, stände einer anschließenden Erhebung personenbezogener Daten nichts im Wege. Das Ministerium fürchtet jedoch einen zusätzlichen Arbeitsaufwand für die Gesundheitsämter; es hält die sofortige personenbezogene Meldung für unerlässlich. Allerdings wurde zugesagt, die Meldungen nach § 34 IfSG nur kurzfristig aufzubewahren und die Daten nicht im automatisierten System zu speichern. Außerdem soll nach einiger Zeit über die praktische Erfahrung mit der personenbezogenen Erhebung berichtet werden.

12.3 Zentrale Begutachtungsstelle für Landesbedienstete

Beim Gesundheitsamt des Stadtverbandes Saarbrücken ist die „Zentrale Gutachtenstelle für Landesbedienstete“ angesiedelt, die aus verschiedenen Anlässen für den Dienstherrn Saarland amtsärztliche Bescheinigungen, Zeugnisse oder Gutachten erstellt.

Auf Anfrage dieser Stelle habe ich mich zu verschiedenen Fragen bezüglich der Datenverarbeitung (insbesondere im Rahmen von Zwangspensionierungsverfahren) geäußert:

- Erforderlichkeit einer Einverständniserklärung für die Weiterleitung von Befunden

  Einer Einverständniserklärung bedarf es meiner Auffassung nach nicht, wenn der im Rahmen des Zwangspensionierungsverfahrens gutachtlich beauftragte Arzt Untersuchungsbefunde an den Dienstherrn weiterleitet.

Gemäß § 4 Saarländisches Datenschutzgesetz ist eine Verarbeitung personenbezogener Daten zulässig, wenn entweder der Betroffene eingewilligt hat oder das Saarländische Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt. Die gesetzliche Befugnis für den Amtsarzt zur Übermittlung der erforderlichen Angaben ergibt sich aus § 52 Abs. 1 Satz 4 Saarländisches Beamtengesetz, wonach dem Dienstherrn die für die Feststellung der Dienstunfähigkeit erforderlichen Untersuchungsergebnisse mitzuteilen sind.

Im Fall der Untersuchung auf Dienstunfähigkeit ist somit für die Übermittlung des Untersuchungsergebnisses an den Dienstherrn eine Einwilligungserklärung des Bediensteten nicht erforderlich. Allerdings kann für Ergebnismitteilungen bei Begutachtungen in anderen Zusammenhängen durchaus eine Einverständniserklärung erforderlich sein. Immer dann, wenn es keine gesetzliche Vorschrift gibt, die die Datenübermittlung erlaubt, bedarf es des Einverständnisses des Begutachteten.

Einer Einverständniserklärung bedarf es somit auch für die Einholung von Auskünften bei den behandelnden Ärzten.

- Umfang der Datenweitergabe an den Dienstherrn

  Dem Dienstherrn sind nach § 52 Abs. 1 Satz 4 SBG die „für die Feststellung der Dienstunfähigkeit erforderlichen Untersuchungsergebnisse mitzuteilen.“ Ich verstehe diese Vorschrift so, dass sich die Aussage im dem ärztlichen Gutachten nicht auf die Feststellung „dienstunfähig“ oder „dienstfähig“ beschränken kann. Andererseits würde ein Gutachten mit Angaben über festgestellte Anamnesedaten oder Einzelbefunde den zulässigerweise zu übermittelnden Umfang überschreiten. Die gutachtliche Äußerung sollte die tragende Begründung enthalten, die der Dienstherr für seine Entscheidung benötigt.

- Zeitpunkt der Unterschrift unter die Einverständniserklärung

  Die Anforderung von Unterlagen bei behandelnden Ärzten kommt nur in Betracht, wenn diese für die Begutachtung durch die zentrale Gutachtenstelle erforderlich sind. Ob eine solche Notwendigkeit besteht, obliegt der Beurteilung durch den begutachtenden Arzt. Erst wenn dieser eine entsprechende Notwendigkeit sieht, wird die Einholung des entsprechenden Einverständnisses des zu Begutachtenden nötig.

  Eine Verfahrensweise, bei der die Einverständniserklärung schon vor der ärztlichen Untersuchung im Zusammenhang mit der Aufnahme der Personalien unterschrieben werden muss, entspricht somit nicht den datenschutzrechtlichen Anforderungen. Auch eine Blanko-Einverständniserklärung, bei der nicht die Namen der Ärzte oder Einrichtungen, bei denen Unterlagen angefordert werden sollen, in dem Formular angegeben

sind, entspricht nicht den Anforderungen an eine rechtswirksame Einwilligung.

12.4 Datenschutzprüfung im Krankenhaus

Die Prüfung in einem Krankenhaus, dessen privatrechtlich organisierter Träger im wesentlichen von der öffentlichen Hand beherrscht wird, habe ich insbesondere auf den Umgang mit Patientendaten bezogen. Dabei habe ich Datenschutzmängel angetroffenen, wie sie in ähnlicher Form auch in anderen Kliniken festzustellen sind, obwohl das Saarländische Krankenhausgesetz (SKHG) bereits im Jahre 1987 spezielle Regelungen hierfür getroffen hat.

Die Zugriffsrechte der Beschäftigten auf die Patientendaten waren zu weit bestimmt. Wie häufig wurden wir mit dem Einwand konfrontiert, alle im Krankenhaus Beschäftigten seien doch zur Geheimhaltung verpflichtet, interne Abschottungsmaßnahmen seien deshalb überflüssig, sie würden den Arbeitsablauf beeinträchtigen und unter Umständen sogar die Behandlung eines Patienten verzögern.

Das Krankenhaus ist jedoch keine informationelle Einheit, in der jeder Mitarbeiter in die Daten aller Patienten Einsicht nehmen darf. § 29 Abs. 3 Satz 2 SKHG legt fest, dass die im Krankenhaus Beschäftigten Patientendaten nur für den zur jeweiligen Aufgabenerfüllung gehörenden Behandlungszweck einsehen oder sonst nutzen dürfen. Medizinische Behandlungsdaten einer Abteilung dürfen grundsätzlich nicht dem Personal einer anderen Abteilung zugänglich sein. Mitarbeiter in der Verwaltung dürfen von medizinischen Daten nur insoweit Kenntnis erhalten, als dies für ihre Aufgaben, insbesondere für die Abrechnung des Behandlungsfalles, erforderlich ist. Funktionsstellen dürfen nur Zugriff auf die Daten erhalten, die sie für ihre Arbeit benötigen.

Durch technische und organisatorische Maßnahmen ist sicherzustellen, dass das Patientengeheimnis gewahrt bleibt. Auch in dem geprüften Krankenhaus wurden diese Regeln nicht strikt eingehalten. Alle Einzelkliniken hatten Zugriff auf die Daten aller Patienten, die seit Einsatzbeginn des Patienteninformationssystems behandelt wurden. Eine Beschränkung der Zugriffsrechte auf die einzelnen Fachbereiche war in dem System zum damaligen Zeitpunkt noch nicht vorgesehen. Ein besonderes Auskunftsmodul enthielt nicht nur Grunddaten über den Patienten (Namen, Adresse, Geburtsdatum, Aufnahme- und Entlassungsdatum, Fachabteilung, Station), wie es etwa für den Empfangsbereich/Pförtner und das Krankenblattarchiv ausreichend gewesen wäre, sondern auch Angaben über Kostenträger, erbrachte Leistungen (z.B. Wahlleistung), Angehörige, Hausarzt und Aufnahmeart (z.B. Notfall, Selbstmordversuch).

Bei der Patientenaufnahme wurden die vorrangig für Verwaltungs- und Abrechnungszwecke erhobenen Daten unmittelbar am Terminal erfasst. Die in der Krankenversichertenkarte gespeicherten Daten wurden automatisiert eingelesen. Ein Aufnahmeformular, das von den Patienten zunächst auszufüllen ist, wurde nicht verwendet. Dieses Verfahren ist zwar praktisch, aber aus datenschutzrechtlicher Sicht insoweit problematisch, als nicht sichergestellt ist, dass die Patienten oder ihre Angehörigen informiert sind, zu welchen Angaben sie verpflichtet sind und welche Daten auf freiwilliger Grundlage erhoben werden. Dabei bestand auch bei dem aufnehmenden Personal Unsicherheit, welche Daten freiwillig angegeben werden können und welche zur Abwicklung des Behandlungsvertrages unerlässlich sind.

Ich habe vorgeschlagen, den Patienten vor der Datenerfassung ein Info-Blatt auszuhändigen, in dem sie aufgeklärt werden, welche Daten aus welchen Gründen auf freiwilliger Basis erhoben werden und in dem sie ihre Einwilligung zur Verarbeitung dieser Daten erklären können. Zusätzlich sollte in der Erfassungsmaske bei den betreffenden Datenfeldern ein Hinweis auf die Freiwilligkeit oder die Voraussetzungen der Erhebung aufgenommen werden (z. B. Arbeitgeber nur, wenn die Versicherungsverhältnisse unklar sind).

Bei der Aufnahme wurde der Patient auch mündlich nach seiner Religionszugehörigkeit gefragt und die Angabe am Terminal erfasst. Patienten, die ihre Religionszugehörigkeit angaben, wurden in die „Pfarrerliste“ aufgenommen, die vom System ausgedruckt und beim Pförtner zur Einsicht für die beiden Krankenhausseelsorger und den Besuchsdienst der Kirchen- bzw. Pfarrgemeinden bereitlag. Oftmals waren Patienten überrascht, dass ihre Gemeinde Kenntnis von der Krankenhausaufnahme hat und dass sie von Helfern aus der Gemeinde besucht werden. Damit die Rechte der Patienten gewahrt werden, ist die Einwilligung entsprechend der Regelung in § 29 Abs. 2 SKHG schriftlich einzuholen. Dabei sollte den Patienten auch das Wahlrecht eingeräumt werden, ob ihre Daten nur dem Krankenhausseelsorger oder auch dem gemeindlichen Besuchsdienst zugeleitet werden sollen. Die „Pfarrerliste“ darf nur dem jeweils zuständigen Krankenhausseelsorger zur Verfügung gestellt werden. Für den gemeindlichen Besuchsdienst sollten - je nach Heimatort - separate Listen angefertigt werden, die nur die Patienten enthält, die hierfür ihre Einwilligung erteilt haben. Das Krankenhaus hat meine Anregungen - auch den Formulierungsvorschlag für einen Passus im Informationsblatt - übernommen.

Auch in dem geprüften Krankenhaus wurden wieder Warnmeldungen der Deutschen Krankenhausgesellschaft über Krankenhauswanderer vorgefunden. Es handelt sich um Personen, die sich in anderen Krankenhäusern durch Vorspiegelung falscher Tatsachen einen stationären Aufenthalt erschwindelt haben. Die Meldungen, in denen die Ereignisse unter Nennung des Namens und weiterer personenbezogener Daten detailliert geschildert

sind, wurden im Bereich der Krankenhausaufnahme für einige Jahre gesammelt und anschließend im Archiv aufbewahrt. Bisher hatte noch keine dieser Personen um stationäre Aufnahme nachgesucht. Die Meldung solcher Fälle durch ein Krankenhaus ist, weil eine gesetzliche Befugnis zur Datenübermittlung fehlt, unzulässig. Überdies halte ich die Warnmeldungen für kein geeignetes Mittel, Missbräuche zu verhindern, weil eventuelle frühere Betrügereien keine Ablehnung der Krankenhausbehandlung rechtfertigen, wenn später tatsächlich einmal akute Behandlungsbedürftigkeit besteht.

Nach § 29 Abs. 5 Satz 1 SKHG sind Patientendaten zu löschen, wenn sie zur Erfüllung der Aufgaben nach Abs. 2 und 3 - also zur Abwicklung des Behandlungsfalles - nicht mehr erforderlich und die durch Rechtsvorschriften oder die ärztliche Berufsordnung vorgeschriebenen Aufbewahrungsfristen abgelaufen sind. Satz 2 schreibt darüber hinaus vor, dass Patientendaten, die im automatisierten Verfahren mit der Möglichkeit des Direktabrufs gespeichert sind, unmittelbar nach Abschluss der Behandlung zu löschen sind. Es darf nur ein Restdatensatz gespeichert bleiben, der für das Auffinden der Krankenakte erforderlich ist.

Die Umsetzung dieser Vorschrift bereitet in der Praxis zunehmend Schwierigkeiten. Ihr liegt die Annahme zugrunde, dass ein automatisierter Datenbestand, auf den jederzeit zugegriffen werden kann, höhere Gefahren für das Patientengeheimnis mit sich bringt als die manuelle Sammlung konventioneller Krankenunterlagen oder auf externen Datenträgern (d.h. nicht direkt abrufbare) elektronisch gespeicherte Informationen. Seit Inkrafttreten des Krankenhausgesetzes sind die technischen Möglichkeiten weiter fortgeschritten; es stehen leistungsfähige Patientenverwaltungssysteme zur Verfügung, die differenzierte Zugriffsbeschränkungen erlauben. Dem gegenüber lässt sich die unzulässige Verarbeitung bei Nutzung externer Datenträger möglicherweise schwerer ausschließen. Daher erscheint fraglich, ob die Vorschrift des § 29 Abs. 5 Satz 2 SKHG noch angemessen ist.

12.5 Datenübermittlung für die Krankenhausplanung

Zur Vorbereitung des am 1. Januar 2001 in Kraft tretenden Krankenhausplanes hatte das Ministerium für Frauen, Arbeit, Gesundheit und Soziales ein privates Institut mit der Erstellung eines Gutachtens beauftragt. Für die Krankenhausplanung sollte dabei nach dem Konzept des Gutachters anders als in der Vergangenheit an konkrete Belegungs- und Behandlungsdaten der Patienten in den einzelnen Einrichtungen angeknüpft werden. Damit stellte sich die Frage, ob und inwieweit hierbei besonders geschützte personenbezogene Daten von Stellen außerhalb des Krankenhauses verarbeitet werden müssen.

Als Grundlage dieses Gutachtens sollten die Krankenhäuser dem Institut die Daten der in einem bestimmten Zeitraum behandelten Patienten in anony-

mer Form zur Verfügung stellen. Nach dem Saarländischen Krankenhausgesetz (§ 5 SKHG) sind die Krankenhausträger verpflichtet, dem für das Gesundheitswesen zuständigen Minister auf Anfrage die Auskünfte zu erteilen, die unter anderem für die Krankenhausplanung erforderlich sind. Ausdrücklich ist bestimmt, dass Auskünfte nur anonymisiert erteilt werden dürfen (§ 5 Abs. 1 Satz 2 SKHG). Der zur Übermittlung vorgesehene Datensatz genügte den Anforderungen an eine ausreichende Anonymisierung. An Patienten identifizierenden Daten sollten nämlich nur übermittelt werden das Geburtsjahr, die vierstellige Postleitzahl und ein zwölfstelliger numerischer Code, der aus Bestandteilen des Vor- und Nachnamens gebildet werden sollte. Bei näherer Überprüfung habe ich allerdings festgestellt, dass der Code das volle Geburtsdatum des Patienten enthielt. Durch meine Intervention ist es gelungen, diesen Fehler noch zu korrigieren.

12.6 Versendung von Krankenhausentlassungsberichten an den Hausarzt

Es ist üblich, dass die Krankenhäuser nach der Krankenhausbehandlung dem Hausarzt einen Entlassungsbericht übersenden, der die im Krankenhaus durchgeführten Behandlungsmaßnahmen und die Entlassungsdiagnose enthält.

Im Hinblick auf die ärztliche Schweigepflicht stellt sich die Frage, unter welchen Voraussetzungen eine solche Information des Hausarztes zulässig ist. Das Saarländische Krankenhausgesetz enthält hierzu die eindeutige Regelung, dass die Übermittlung von Patientendaten zur Durchführung der Mit- und Nachbehandlung (also auch an den Hausarzt) nur zulässig ist "soweit der Patient nach Hinweis nicht etwas anderes bestimmt. " (§ 29 Abs. 4 Nr. 1 SKHG).

Im Berichtszeitraum habe ich bei den meiner Kontrolle unterliegenden Krankenhäusern nachgefragt, in welcher Weise in Ihrem Hause jeweils die Beteiligung des Patienten bei der Versendung von Entlassungsberichten sichergestellt ist.

Es wurden verschiedene Möglichkeiten genannt, wie die genannte Vorschrift - nach Auffassung der Krankenhäuser korrekt - umgesetzt wird:

- Hingewiesen wurde auf einen Passus im Behandlungsvertrag, wonach der Patient erklärt, er habe Kenntnis davon genommen, dass personenbezogene Daten auf gesetzlicher Grundlage verarbeitet werden.
- Andere Krankenhäuser haben geantwortet, dass es ein spezielles Verfahren für solche Hinweise nicht gebe. Die ganzheitliche Behandlung eines Patienten durch verschiedene medizinische Leistungserbringer, wie beispielsweise Hausarzt, Facharzt, Krankenhaus machen nur einen

Sinn, wenn die Behandlungskette nicht durchbrochen, sondern aufrecht erhalten bleibe.

- Bei der Aufnahme werde der Hausarzt erfragt.
- Man gehe von dem stillschweigenden Einverständnis des Patienten aus.

Die geschilderten Verfahrensweisen sind meines Erachtens nicht geeignet, der gesetzlichen Vorgabe im Saarländischen Krankenhausgesetz Rechnung zu tragen. Ein datenschutzrechtlich korrektes Verfahren wäre es, wenn der Patient beim Entlassungsgespräch über die beabsichtigten Adressaten des Arztbriefes und die Möglichkeit informiert würde, etwas anderes zu bestimmen.

Ich habe die Krankenhäuser gebeten, zukünftig entsprechend zu verfahren.

12.7 Einsichtsrecht des Patienten in ärztliche Dokumentationen

Im Berichtszeitraum legte die Ärztekammer des Saarlandes den Entwurf zur Neufassung der Berufsordnung für die Ärztinnen und Ärzte des Saarlandes vor. Das Ministerium für Frauen, Arbeit, Gesundheit und Soziales hat mich um eine Stellungnahme aus datenschutzrechtlicher Sicht gebeten.

Zum Einsichtsrecht des Patienten in seine beim niedergelassenen Arzt geführten Krankenunterlagen sah der Entwurf folgende Regelung vor:

"Der Arzt hat dem Patienten auf dessen Verlangen grundsätzlich in die ihn betreffenden Krankenunterlagen Einsicht zu gewähren; ausgenommen sind diejenigen Teile, welche subjektive Eindrücke oder Wahrnehmungen des Arztes enthalten."

Zwar habe ich begrüßt, dass erstmals in die Berufsordnung eine Regelung aufgenommen werden sollte, wonach der Arzt dem Patienten auf dessen Verlangen grundsätzlich in die ihn betreffenden Krankenunterlagen Einsicht zu gewähren hat. Wie Patientenbeschwerden belegen, ist dies nämlich leider immer noch keine Selbstverständlichkeit.

Für unvereinbar mit der geltenden Rechtslage halte ich allerdings, dass hierbei diejenigen Teile ausgenommen sein sollen, welche subjektive Eindrücke oder Wahrnehmungen des Arztes enthalten. Diese Einschränkung des Einsichtsrechts des Patienten widerspricht der Regelung in § 34 Bundesdatenschutzgesetz, die ein uneingeschränktes Auskunftsrecht des Betroffenen gegenüber nicht-öffentlichen Stellen, wozu auch die niedergelassenen Ärzte gehören, normiert. Berufsordnungen als Satzungen haben gesetzliche Regelungen als höherrangige Rechtsnormen zu beachten. Deshalb kann die Berufsordnung zu Eingriffen in das informationelle Selbstbestimmungsrecht nicht ermächtigen, soweit dies nicht in Einklang mit dem Bundesdatenschutzgesetz steht.

Im übrigen sind nach meiner Überzeugung Auslegungsschwierigkeiten hinsichtlich der Abgrenzung objektiver von subjektiven Daten vorprogrammiert, so dass zu befürchten ist, dass im Zweifel die Einsichtnahme verweigert wird, wenn die Berufsordnung bei subjektiven Daten eine Versagung des Einsichtsrechtes vorsieht. Probleme kann ich mir insbesondere vorstellen bei der Einordnung der Diagnose; dabei steht für mich außer Frage, dass die Diagnose und auch die Verdachtsdiagnose objektive medizinische Daten sind, die nicht von der Informationspflicht des Arztes ausgenommen sind und auch nicht ausgenommen werden dürfen. Denn die Diagnosen sind zentrale Grundlage der Behandlung; ohne Kenntnis der Diagnose wäre z. B. auch das Aufdecken von Behandlungsfehlern vielfach in Frage gestellt. Deshalb hat sich mir die Frage gestellt, welche Daten überhaupt denkbar sind, die nicht zur Kenntnisnahme des Patienten bestimmt sein sollen.

Große Vorbehalte habe ich auch hinsichtlich der Umsetzung der Regelung in der Praxis geltend gemacht, wenn, wie es wohl der Regelfall sein wird, auf einer Karteikarte sowohl objektive Befunde als auch subjektive Wahrnehmungen des Arztes enthalten sind. Das Ergebnis kann nicht sein, dass bei dieser Fallkonstellation die Einsichtnahme insgesamt verweigert wird. Als Möglichkeit käme nur in Betracht, dass die Aufzeichnungen mit subjektiven Eindrücken abgedeckt werden. Dass eine solche Verfahrensweise dem Vertrauensverhältnis zwischen Arzt und Patienten nicht förderlich wäre, liegt meines Erachtens auf der Hand.

Ein weiterer Gesichtspunkt, der für ein uneingeschränktes Einsichtsrecht spricht, ist, dass nach der Rechtssprechung des Bundesgerichtshofs die Übergabe von Patientenunterlagen bei einem Praxisverkauf der Einwilligung der betreffenden Patienten bedarf. Eine wirksame Einwilligung in diesem Zusammenhang setzt voraus, dass der Einwilligende Kenntnis vom Inhalt der Unterlagen hat oder sich jedenfalls verschaffen kann, in deren Weitergabe er einwilligt. Diese Kenntnis kann nur durch eine umfassende Einsichtsgewährung in die Behandlungsunterlagen vermittelt werden.

Schließlich habe ich auf eine Diskrepanz zwischen der Formulierung in der Entwurfsfassung der Berufsordnung und bestehenden gesetzlichen Regelungen hingewiesen. So enthält die Vorschrift des § 29 Abs. 7 des Saarländischen Krankenhausgesetzes, die die Einsichtnahme in die Behandlungsdokumentation des Krankenhauses regelt, keine Einschränkung im Sinne der beabsichtigten Novellierung der Berufsordnung. Einen Grund für die unterschiedliche Behandlung dieser Frage, je nachdem, ob die Behandlungsunterlagen in einem Krankenhaus oder durch einen niedergelassenen Arzt geführt werden, vermag ich nicht zu erkennen. Da die Berufsordnung auch für Krankenhausärzte gilt, wären hier Schwierigkeiten in der Praxis vorprogrammiert.

Ich hoffe, dass das zuständige Ministerium sich meiner Argumentation anschließt und die Änderung der Berufsordnung in diesem Punkt nicht genehmigt.

12.8 Ärztekammer des Saarlandes

Die Datenschutzprüfung bei den Abteilungen Ärzte, Zahnärzte und Versorgungswerk der Ärztekammer erstreckte sich vorwiegend auf technische und organisatorische Aspekte sowohl im Bereich der EDV als auch im konventionellen Bereich.

So habe ich z. B. vorgeschlagen, einen Geschäftsverteilungsplan aufzustellen, den Zugang zu den Datensammlungen besser zu sichern und bei der Datenträgervernichtung eine höhere Sicherheitsstufe vorzusehen. Außerdem war festzustellen, dass noch immer nicht die im Saarländischen Heilberufekammergesetz vorgesehene Meldeordnung erlassen ist, die den Umfang der von den Kammermitgliedern bei der Meldung anzugebenden Daten und vorzulegenden Unterlagen, den Umfang der Datenweitergabe bei einer Verlegung der Tätigkeit der Kammermitglieder sowie die Dauer der Speicherung der Daten über die Kammermitglieder regeln soll. Das automatisierte Ärzteregister enthielt auch Datenfelder, die für die Aufgabenerfüllung der Kammer nicht erforderlich sind (genauer Familienstand, Angaben über Ehegatten und Kinder).

Die Adresse jedes neuen Kammermitglieds wird an den Verlag des Deutschen Ärzteblattes und den Verlag des Saarländischen Ärzteblattes übermittelt. Die neuen Kammermitglieder erhalten zwar einen Hinweis über die Zusendung des Deutschen Ärzteblattes und des Saarländischen Ärzteblattes. Da eine gesetzliche Übermittlungsbefugnis nicht besteht, ist es jedoch notwendig, vor der Weitergabe der Adressen an die Verlage die schriftliche Einwilligung der Kammermitglieder einzuholen.

Die von den übrigen Organisationseinheiten räumlich getrennte Abteilung Zahnärzte teilt sich nicht nur mit der Kassenzahnärztlichen Vereinigung (KZVS) ein Gebäude; beide Körperschaften des öffentlichen Rechts sind auch personell und bei der Aufgabenerfüllung, insbesondere der Datenverarbeitung, eng miteinander verbunden. So sind die Geschäftsführer in der jeweils anderen Körperschaft als stellvertretende Geschäftsführer tätig; es wird eine gemeinsame Datenbank der Zahnärzte für die unterschiedlichen Aufgaben der beiden Körperschaften geführt; die EDV-Systemverwaltung, die Finanzbuchhaltung und die Personalabrechnung werden von der KZVS erledigt. Ärztekammer und KZVS sind öffentliche Stellen, denen vom Gesetzgeber (SHKG, SGB V) unterschiedliche Aufgaben übertragen sind. Der Kreis der betroffenen Zahnärzte ist zwar bei beiden Institutionen überwiegend identisch (von ca. 830 Zahnärzten der Ärztekammer gehören ca. 730 der KZVS an). Dennoch ist aus datenschutzrechtlicher Sicht klarzustellen,

welche Körperschaft für die Verarbeitung welcher Daten verantwortlich ist, welche damit „Herr der Daten“ ist, gegen wen sich Datenschutzrechte wie Ansprüche auf Auskunft, Berichtigung und Löschung richten, wer welche Weisungsbefugnisse gegenüber dem Systemverwalter hat, welche Körperschaft auf welche Daten zugriffsberechtigt ist, welche für Schadenersatzansprüche bei etwaiger unzulässiger oder unrichtiger Verarbeitung haftet usw. Ich habe verlangt, dass zwischen Ärztekammer und KZVS schriftliche Regelungen über Aufgabenverteilung und Abgrenzung der Verantwortlichkeiten bei der Datenverarbeitung getroffen werden.

Die Ärztekammer hat zugesichert, meine Forderungen zu erfüllen.

12.9 Saarbrücker Drogenhilfezentrum

Das Saarbrücker Drogenhilfezentrum hat im Berichtszeitraum einen sogenannten Druckraum eröffnet, in dem volljährige und langjährig drogenabhängige Personen Drogen konsumieren dürfen.

In einer „Umsetzungskonzeption zur Einrichtung eines Druckraums“ hat das Ministerium für Frauen, Arbeit, Gesundheit und Soziales festgelegt, dass das Projekt während der Erprobungsphase jährlich dokumentiert wird, um zu überprüfen, ob die mit der Einrichtung des Druckraums verfolgten Ziele erreicht werden.

In (vermeintlicher) Umsetzung dieser Anforderung hat das Drogenhilfezentrum einen Nutzungsantrag entwickelt, in dem der Nutzer neben Namen und sonstigen Personalien auch Angaben zu seinem zurückliegenden und gegenwärtigen Drogenkonsumverhalten machen muss.

Wenngleich hiervon das Drogenzentrum selbst für seine Arbeit Kenntnis haben muss, war für mich nicht nachvollziehbar, inwiefern eine – anderen Stellen zuzuleitende - Dokumentation des Projekts zwingend die Verarbeitung personenbezogener Daten der Nutzer des Druckraumes erforderlich machen sollte. Mir erschien vielmehr zu diesem Zweck eine Erfassung in anonymisierter Form ausreichend.

Das Ministerium ist meinen Bedenken gefolgt und hat einen Erhebungsbogen vorgelegt, in dem der Name des Drogenabhängigen nicht mehr erfasst wird. Ob durch das Weglassen des Namens die Möglichkeit einer Wiederherstellung des Personenbezuges ausgeschlossen ist, ist derzeit noch Gegenstand von Erörterungen mit dem Ministerium.

12.10 Saarländisches Krebsregistergesetz

Dass das Saarländische Krebsregistergesetz – trotz der unbezweifelbaren Verdienste, die das auf dessen Grundlage eingerichtete Register für die wissenschaftliche Forschung hat – nicht den Anforderungen des Datenschutzes

entspricht und im übrigen auch nicht hinreichend den Belangen der Forschung genügt, steht in nahezu jedem der bislang vorgelegten Tätigkeitsberichte. Die Verpflichtung aller Bundesländer durch den Bundesgesetzgeber, für derartige Register Rechtsgrundlagen zu schaffen, hat hieran nichts geändert. Zur notwendigen umfassenden Novellierung des Saarländischen Krebsregistergesetzes kam es nicht. Zwar hatte die frühere Landesregierung schließlich den Entwurf einer Teilregelung in den Landtag eingebracht; er ist dort jedoch nicht weiter verfolgt worden und letztlich der Diskontinuität zum Opfer gefallen.

Bei der Neuordnung der Geschäftsbereiche in der neugebildeten Landesregierung wurde das Krebsregister vom Statistischen Amt zum Gesundheitsministerium verlagert. Diese Organisationsänderung sehe ich eher als Rückschritt gegenüber der vorherigen Rechtslage; die Einbeziehung in die Fachverwaltung mit deren möglicherweise speziellen Interessen und die nunmehr noch betonte organisatorische Verzahnung mit gesonderten Studien widerspricht meines Erachtens einer angemessenen Abschottung für die Behandlung höchst sensibler personenbezogener Daten.

Ich habe dies zum Anlass genommen, in einer Presseerklärung „Endlich neue Rechtsgrundlage für Krebsregister schaffen!“ erneut einen Vorstoß zur längst fälligen Novellierung des Saarländischen Krebsregistergesetzes zu unternehmen. In einer Besprechung mit Vertretern des Ministeriums für Frauen, Arbeit, Gesundheit und Soziales wurde die Vorlage eines entsprechenden Entwurfes zugesagt. Geschehen ist allerdings bis heute nichts. Bei allem Verständnis dafür, dass die inzwischen abgeschlossene Studie zum Abgleich von Fallmeldungen nach dem Bundeskrebsregistergesetz ausgewertet werden muss, ist ein weiteres Zuwarten nicht mehr vertretbar, zumal seit Beginn der Diskussion um eine Novellierung des Saarländischen Krebsregistergesetzes nunmehr bereits 15 Jahre vergangen sind. Wenn nicht die Parlamentarier selbst sich des Themas annehmen, bleibt es bei der wenig durchsichtigen Datenübermittlung hinter dem Rücken der Patienten und nur spärlichen Sicherungen für das Register, dem bei strenger Auslegung des geltenden Rechts wichtige Beiträge für sinnvolle medizinische Forschung verwehrt sind. Den Beginn des letzten Forschungsvorhabens, bei dem ich beteiligt wurde, konnte ich nur in der Erwartung akzeptieren, dass für den später notwendigen Abgleich mit dem Krebsregister die gesetzlichen Voraussetzungen geschaffen werden.

13 Forschung

13.1 Epidemiologische Studie zu chronischen Erkrankungen in der älteren Bevölkerung (ESTHER)

Im Berichtszeitraum hat mich das Ministerium für Frauen, Arbeit, Gesundheit und Soziales um eine datenschutzrechtliche Stellungnahme zu einer epidemiologischen Studie gebeten, die zusammen mit dem Deutschen Zentrum für Altersforschung in Heidelberg durchgeführt wird.

Personen im Alter zwischen 50 und 74 Jahren sollen auf freiwilliger Basis einen Fragebogen zu ihrem Gesundheitszustand ausfüllen und in die Durchführung verschiedener Laboruntersuchungen einwilligen. Ziel der Studie ist es, eine verbesserte Verhütung, Früherkennung und Therapie chronischer Erkrankungen in der älteren Bevölkerung in Deutschland zu erreichen.

Nach Prüfung des sorgfältig erarbeiteten Datenschutzkonzeptes musste ich keine grundsätzlichen datenschutzrechtlichen Bedenken geltend machen. Es gab allerdings auch Punkte, die teilweise kontrovers diskutiert wurden:

- Es war vorgesehen und wird heute auch so praktiziert, dass den Patienten in der Arztpraxis ein Informationsblatt, eine Einverständniserklärung und der Fragebogen ausgehändigt wird. Die Patienten sollen noch während des Arztbesuches die Einverständniserklärung unterschreiben und den Fragebogen ausfüllen.

  Ich habe Zweifel geäußert, ob bei dieser Verfahrensweise noch von einer wirksam erteilten Einverständniserklärung des Patienten ausgegangen werden kann, weil er in der Kürze der Zeit die komplexen Datenverarbeitungsvorgänge wohl kaum überschauen kann. Allerdings konnte ich mich mit diesen Bedenken nicht durchsetzen. Die Studienleitung war der Ansicht, dass der Patient während der Wartezeit genügend Zeit habe, das Informationsblatt und die Einverständniserklärung durchzulesen. Außerdem stehe es jedem Patienten grundsätzlich frei, die Unterlagen mit nach Hause zu nehmen und dann über eine Teilnahme zu entscheiden. Auch sei zu jeder Zeit ein Rücktritt mit vollständiger Vernichtung aller bis dahin erhobener Daten möglich.

- Das Datenschutzkonzept sieht vor, dass die Fragebögen mit Name und Adresse des jeweiligen Patienten bei dem Studienzentrum eingehen. Dies deshalb, um gegebenenfalls Rückfragen bei unvollständigen Angaben durchführen zu können. Aus dem Informationsblatt für die Patienten ging diese Tatsache meines Erachtens nicht mit hinreichender Deutlichkeit hervor. Das Informationsblatt wurde daraufhin entsprechend meinem Formulierungsvorschlag geändert.

- Vorgesehen war, dass mit Einverständnis der Teilnehmer deren Eigenangaben durch Informationen des Saarländischen Krebsregisters verifiziert bzw. ergänzt werden.

  Hier musste ich darauf hinweisen, dass die Verwendung von Daten des Krebsregisters für die Studie sich strikt an den Vorgaben des Saarländischen Krebsregistergesetzes orientieren muss, und dass auch eine Einwilligung Datenverarbeitungsvorgänge nicht legitimieren kann, die mit dem Saarländischen Krebsregistergesetz nicht vereinbar sind.

13.2 Genomanalyse

Bei der Entschlüsselung des menschlichen Genoms sind in den letzten Monaten entscheidende Durchbrüche gelungen. Von der Entschlüsselung des Erbguts erhoffen sich die Wissenschaftler unter anderem, die Ursachen schwerer Krankheiten zu erkennen und besser behandeln zu können.

Der Umgang mit genetischen Daten birgt aus der Sicht des Datenschutzes allerdings schwerwiegende Risiken. Gegenüber anderen Gesundheitsdaten weisen sie gerade im Hinblick auf das informationelle Selbstbestimmungsrecht Besonderheiten auf. So ist "Betroffener" bei genetischen Daten nicht nur diejenige Person, deren DNA untersucht wird, betroffen sind zugleich die Blutsverwandten, die von der Genomuntersuchung möglicherweise gar nichts wissen wollen.

Hinsichtlich der Gesundheit eines Menschen geben Gene in aller Regel nur Auskunft über Dispositionen zu bestimmten Krankheiten. Der tatsächliche Eintritt der Krankheit hängt meist von vielen weiteren Faktoren ab. Aussagen über genetische Anlagen sind als Daten inhaltlich also viel unbestimmter als eine Krankheitsdiagnose. Genetische Daten über Krankheitsanlagen prägen das Lebensgefühl eines Menschen von der Kenntnis bis zum Tod. Das gilt auch für den Fall, dass die Anlage sich nicht manifestiert, die betroffene Person also gesund bleibt. Das Genom enthält ein umfassendes Persönlichkeitsprofil des Betroffenen, auch wenn es zur Zeit nur teilweise entschlüsselt werden kann. Herkömmliche Gesundheitsdaten beschränken sich dagegen auf bestimmte Teilinformationen zur Person. Schließlich können Ergebnisse von Genomanalysen im Gegensatz zu herkömmlichen Gesundheitsdaten nicht vollständig anonymisiert werden.

Diese Besonderheiten von genetischen Daten gebieten eine besondere datenschutzrechtliche Behandlung. Dem kann gegenwärtig zwar vielfach durch eine entsprechende Interpretation der datenschutzrechtlichen Vorschriften Rechnung getragen werden; klare Spezialregelungen wären jedoch wünschenswert.

Dies gilt z.B. für Arbeits- und Versicherungsverhältnisse. So sollte der Bewerber um einen Arbeitsplatz davor geschützt werden, dass er sich auf Ver-

anlassung des Arbeitgebers zur Verbesserung seiner Chancen einem "freiwilligen" Gentest unterzieht. Ein klares Verbot für Arbeitgeber, Gentests von Bewerbern zu verlangen und entgegenzunehmen, könnte dem Rechnung tragen.

Entsprechendes gilt für die Anbahnung von Versicherungsverhältnissen. Hier besteht die Gefahr einer gesellschaftlichen Diskriminierung, wenn Interessenten für eine Lebensversicherung regelmäßig von sich aus günstige Genomanalyse-Ergebnisse vorlegen und damit indirekt die schlechten Risiken bzw. die ungetesteten Antragsteller in die Defensive drängen.

Bereits 1989 hatten die Datenschutzbeauftragten des Bundes und der Länder sich mit einigen Grundsätzen zur Problematik geäußert, die die Genomanalyse für das Recht auf informationelle Selbstbestimmung aufwirft. Die fortschreitende Entwicklung hat die Konferenz der Datenschutzbeauftragten auf ihrer Tagung am 12. und 13. Oktober 2000 veranlasst, eindringlich nochmals darauf hinzuweisen, dass für die Zulässigkeit gentechnischer Untersuchungen beim Menschen und für den Umgang mit den dabei gewonnenen Informationen sehr schnell klare und verbindliche Prinzipien entwikkelt werden müssen (Anlage 24).

Sie werden weiterhin auch ihrerseits versuchen, wesentliche Gesichtspunkte in die Diskussion um ethische, rechtliche und technische Leitlinien und Schranken mit einzubringen.

14 Schulen

14.1 Internet - und EDV – Einsatz an Schulen

„EDV-Einsatz, Multimediales Lernen, Internet und Netzwerke sind inzwischen zu Realitäten unserer modernen Gesellschaft und damit auch der Schulen geworden, denen wir uns nicht mehr verschließen können“ so lautete ein treffendes Zitat aus der Schülerzeitung des Hochwaldgymnasiums Wadern. Diese Entwicklung wird durch verschiedene Initiativen (z. B. „Schulen ans Netz“, „Smiley-Award“, „Zukunft schenken“, „PC-Führerschein“, „Lehren für die Zukunft“) insbesondere auch von der Landesregierung gezielt gefördert und führt dazu, dass sich der EDV-Einsatz und die Internet-Nutzung lawinenartig in den Schulen ausbreiten.

Über die technische Hilfe bei der Erledigung der Verwaltungsaufgaben hinaus sind es die Einsatzmöglichkeiten im oder im Zusammenhang mit dem Unterricht, zur internen und externen Kommunikation sowie zur Darstellung nach außen, die an den Schulen Interesse finden und ausprobiert werden. Die Nutzung neuer, leistungsfähiger Informations- und Kommunikationstechniken sieht man insoweit vorrangig unter technischem oder pädagogisch-didaktischem Aspekt. Dabei werden aber häufig datenschutzrechtliche

Risiken nicht vollständig erkannt und bestehende rechtliche Bestimmungen zu wenig beachtet. Dies gilt auf allen Ebenen: selbst das Kultusministerium hat den Preis im Wettbewerb „Smiley-Award“ an Internet-Angebote von Schulen (Homepages) vergeben, ohne die datenschutzrechtlichen Anforderungen zu berücksichtigen.

Um mir einen Eindruck über die aktuelle Situation zu verschaffen und Vorschläge für die datenschutzgerechte Realisierung der Anforderungen machen zu können, habe ich eine datenschutzrechtliche Querschnittsprüfung durch die verschiedenen Schulformen vorgenommen, die ich allerdings auf die EDV-Nutzung beschränkt habe. Durch Vorortprüfung von je einer ausgewählten Schule aus den 6 verschiedenen Schulformen (Grundschule, Erweiterte Realschule, Sekundarschule, Gesamtschule, KBBZ, Gymnasium) sollte ein Bild über den datenschutzrechtlichen Stand in den Schulen und das entsprechende Problembewusstsein bei den Lehrkräften entstehen.

Als Ergebnis kann ich allgemein feststellen:

14.1.1 Problembewusstsein und Kenntnisstand

In allen geprüften Schulen haben sich sehr engagierte Lehrer durch Fortbildung und Literaturstudium umfangreiche Kenntnisse erarbeitet und, teilweise mit Unterstützung fachkundiger Eltern oder Firmen, Computer-Installationen vorgenommen und (z. T. sogar vernetzte) Internet-Zugänge realisiert. Wie zu erwarten war, wurde bezüglich des Datenschutzes ein umfassendes Spektrum - von Minimalerfüllung bis hin zu fast vollständiger Erfüllung - der entsprechenden Anforderungen angetroffen. Dies hängt selbstverständlich auch ab von dem datenschutzrechtlichen Kenntnisstand und Problembewusstsein der handelnden Personen (Lehrer, Schüler, Eltern, Schulaufsicht), der Größe und Finanzkraft der Schule und ihrer personellen und räumlichen Ausstattung. Einen entscheidenden Einfluss haben auch die bisherigen Vereinheitlichungsbemühungen des Ministeriums bezüglich Schulverwaltungssoftware (z. B. BBZ, SEKI, Winschool), da damit für die „formalen“ datenschutzrechtlichen Pflichten (Freigabe, Dienstanweisung und Meldung zum Dateienregister) Muster vorliegen und einfacher umzusetzen waren.

In den Schulen werden an personenbezogenen Daten im Wesentlichen Schülerdaten und Lehrerdaten verarbeitet, daneben auch Daten von Erziehungsberechtigten und Mitgliedern der Mitbestimmungsgremien. Es war nur teilweise bewusst, dass dies den Regelungen des SDSG und der Verordnung des Bildungsministeriums über die Erhebung, Verarbeitung und sonstigen Nutzung personenbezogener Daten in den Schulen vom 3.11.1986 unterliegt.

Besondere Unsicherheit war festzustellen, wenn es um das Einstellen personenbezogener Angaben in etwaige Internet-Angebote ging; spezielle Informationen fehlten, auch mein Merkblatt über Anforderungen an Internet-Angebote und die Internet-Nutzung öffentlicher Stellen war nicht bekannt. Bei der Erörterung der Problematik wurde von Seiten der Schulen mehrfach darauf verwiesen, dass in Internet-Seiten enthaltene Daten schon in (lokalen) Informationsblättern, Broschüren, Schülerzeitungen, Telefonbüchern und Zeitungen veröffentlicht sind; übersehen wurde dabei jedoch, dass mit der automatisierten Verarbeitung, die durch die Funktionalität von Suchmaschinen besondere Bedeutung erhält, wesentlich höhere Risiken für das informationelle Selbstbestimmungsrecht der Betroffenen entstehen.

14.1.2 Prüfergebnisse

Aus dem Saarländischen Datenschutzgesetz folgt insbesondere, dass

- die Verfahren mit der Verarbeitung personenbezogener Daten vor ihrem erstmaligen Einsatz und einer wesentlichen Änderung formell freizugeben sind (§ 8 Abs. 2 SDSG)

  Ergebnis: nur zu einem Teil der Verfahren gab es diese Freigabe (z. B. BBZ, SEKI, Winschool); bei keinem der Internet-Angebote konnte eine Freigabe festgestellt werden, da den Schulen die datenschutzrechtliche Relevanz nicht bekannt war

- der Landesbeauftragte für Datenschutz vor der Freigabe von Verfahren (§ 8 Abs. 2 SDSG) und der Inkraftsetzung von Verwaltungsvorschriften (§ 8 Abs. 1 SDSG) zu hören ist

  Ergebnis: wie oben

- die Verarbeitung von personenbezogenen Daten nur auf gesetzlicher Grundlage oder mit Zustimmung des Betroffenen erlaubt ist (§ 4 Satz 1 SDSG), wobei die Einwilligung grundsätzlich der Schriftform bedarf (§ 4 Satz 2 SDSG)

  Ergebnis: Gerade bei den Internet-Angeboten lagen keine schriftlichen Zustimmungen vor; teilweise waren die Zustimmungen mündlich eingeholt worden

- bei der Gestaltung und dem Einsatz von Verfahren technische und organisatorische Anforderungen zur Sicherstellung des Datenschutzes zu erfüllen sind (§11 SDSG)

  Ergebnis: Insgesamt war die Wirksamkeit der festgestellten Datensicherungs- und Datenschutzmaßnahmen beim EDV-Einsatz und insbesondere bei Internet-Angeboten höchst unterschiedlich. Die getroffenen Maßnahmen beruhten auf dem jeweiligen Kenntnisstand der betreuenden Lehrer, die sich zwar bemüht haben, Risiken auszuschalten, doch unsi-

cher waren, ob die getroffenen Maßnahmen ausreichen; Hausmeister und Putzfrauen besaßen Generalschlüssel und hatten damit unkontrolliert Zugang zu allen Anlagen; Kontrollen erfolgten mit wenigen Ausnahmen durch den Systemverwalter, der sich damit selbst kontrolliert (eine Funktionstrennung besteht nicht); Passworte waren nicht benutzerspezifisch und zu kurz; die BIOS-Konfiguration war teilweise nicht sicher genug

- eine Auftragsdatenverarbeitung vertraglich geregelt sein muss, wobei sich der Auftragnehmer den Bestimmungen des SDSG und der Kontrolle des LfD unterwerfen muss (§ 5 SDSG)

  Ergebnis: Auftragsdatenverarbeitung stellten wir lediglich bei Internet-Angeboten fest. Nur in wenigen Fällen konnten aber schriftliche Verträge vorgelegt werden, in der Regel firmenspezifische Vertragsmuster ohne Beachtung des § 5 SDSG. Aus Kostengründen gab es auch Internet-Angebote auf Servern bei Billig-Dienstleistern, wobei die Nutzung per Internet-Anmeldung erfolgte und eine Dokumentation bzw. Verträge nicht vorliegen.

- für jedes Verfahren eine Meldung zum Dateienregister abzugeben ist (§ 23 i. V. m. § 9 SDSG)

  Ergebnis: wie bei Freigabe und Beteiligung des LfD

Aus der Verordnung des MBKW folgt unter Anderem, dass

- bezüglich personenbezogener Daten eintragungs- und einsichtsberechtigte Personen auf das Datengeheimnis zu verpflichten und über die Datensicherung zu belehren sind (§ 3 Abs. 1 Satz 3 der VO; die Verordnung sieht noch immer eine Verpflichtung - im Sinne des alten Datenschutzgesetzes - vor, die im Interesse einer besseren Information wie im aktuellen SDSG durch eine Unterrichtung ersetzt werden sollte)

  Ergebnis: nur teilweise lagen schriftliche Verpflichtungserklärungen vor

- personenbezogene Daten nur auf den in der Schule befindlichen oder auf anderen automatischen Datenverarbeitungsanlagen des Schulträgers verarbeitet werden dürfen (§ 5 Satz 1 der VO)

  Ergebnis: aufgrund der personellen und technischen Gegebenheiten wurden teilweise Daten auf privaten Anlagen verarbeitet (z. B. Zeugnisse, Stundenpläne). Von Schulleitern wurde darauf hingewiesen, dass dieses Verbot der inzwischen eingetretenen technischen Entwicklung und der Situation an den Schulen nicht Rechnung trage.

- Verwaltungsarbeiten nur mit einem ausschließlich dafür bestimmten, nicht auch im Rahmen des Unterrichts verwendeten Rechner und unver-

netzt mit anderen Anlagen ausgeführt werden dürfen (§ 5 Satz 3 Nr. 1 a und b der VO)

Ergebnis: auch für Verwaltungsarbeiten war die Verarbeitung in Verwaltungsnetzen vorgesehen, denen die Verordnung noch nicht Rechnung trägt; sachlich wäre aus Sicht des Datenschutzes gegen eine Nutzung in Rechnernetzen nichts einzuwenden, so lange das Verwaltungsnetz vom Unterrichtsnetz getrennt ist

- Probe- und Fehldrucke vollständig und zuverlässig zu vernichten sind (§ 5 Satz 3 Nr. 1 f der VO)

  Ergebnis: in allen Schulen befanden sich Aktenvernichter, die lediglich Streifen schneiden; die nach der Richtlinie des MdI (GMBl 1989 S. 2) geforderte Sicherheitsstufe S4 (Schnipsel) wurde nirgends erreicht

- Sicherungskopien zu ziehen sind, die gesondert aufzubewahren und vor dem Zugriff Unbefugter zu sichern sind (§ 5 Satz 3 Nr. 2 der VO)

  Ergebnis: wegen fehlender Sicherungsmöglichkeiten wurden teilweise Sicherungskopien privat unter Kontrolle gehalten und aufbewahrt

- im Unterricht eingesetzte automatische Anlagen nicht für außerunterrichtliche Zwecke verwendet werden dürfen (§5 Satz 3 Nr. 2 der VO)

  Ergebnis: teilweise wurden die schulischen Anlagen für VHS-Kurse genutzt, so dass die auf den Rechnern liegenden Daten von Unbefugten zur Kenntnis genommen werden können

- die Übermittlung von Daten an Einzelpersonen oder private Einrichtungen ohne Einwilligung des Erziehungsberechtigten oder des volljährigen Schülers nur zulässig ist, soweit dies zur Erfüllung der Aufgaben der Schule erforderlich ist; ansonsten ist eine entsprechende Einwilligung einzuholen (§ 7 Abs. 1 Satz 1 der VO)

  Ergebnis: Insbesondere die Internet-Angebote, die einer völlig unbestimmten Vielzahl fremder Personen zugänglich sind, enthielten umfangreiche personenbezogene Daten (Lehrer und ihre Unterrichtsbefähigung bzw. Sprechstunden bis hin zu Bildern; Schüler und ihre Klassen-, Kurs- , AG-Zugehörigheit, Prüfungsergebnisse; Elternsprecher und Fördervereine, Hausmeister und Sekretariatskräfte). In keinem Falle lag hierzu eine schriftliche Einwilligungserklärung vor, allenfalls wurde das Einverständnis mündlich durch Anfrage an eine Gruppe eingeholt. Gästebücher enthielten kritische Daten und erfordern permanente Kontrolle.

14.1.3 Folgerungen

Bei den geprüften Schulen stieg mit Vermittlung der gesetzlichen Anforderungen und der Risiken der Internet-Nutzung das datenschutzrechtliche

Problembewusstsein stark an. Alle Schulen waren bereit, ihre neuen Erkenntnisse auch in die Tat umzusetzen, und schlugen schon von sich aus konkrete Maßnahmen vor. Einzelne Maßnahmen wurden inzwischen schon umgesetzt bzw. eingeleitet.

Anzunehmen ist aber, dass die ursprünglich festgestellten Defizite auch in den meisten übrigen Schulen vorhanden sind und sich bei verstärkter Ausstattung mit EDV-Anlagen und Forcierung der EDV- und Internet-Nutzung noch verschärfen, da die hierfür derzeit zuständigen Personen meist nicht ausreichend qualifiziert sind oder schnell genug qualifiziert werden können, für die Schulen aber ausgebildetes anderes Personal regelmäßig nicht verfügbar ist. Ob die Schulträger hier einspringen können, dürfte fraglich sein, da deren Personal- und Finanzlage öffentlich beklagt wird und eine optimale Betreuung aller Schulen vermutlich umfangreiche, nicht realisierbare Stellenausweitungen zur Folge hätte. Insofern wäre wohl eine Unterstützung durch leistungsfähige, vertrauenswürdige DV-Dienstleister vor Ort eine gangbare Alternative.

Vor allem wurde bei der Prüfung aber deutlich, dass dringender Schulungs-, Informations-, Koordinations- und Beratungsbedarf besteht. Hierum sollte sich primär die Schulaufsicht kümmern. Auswirkungen, die sich auf die Schulträger ergeben, müssten mit diesen abgestimmt werden.

Als notwendigen ersten Schritt, auf den das Ministerium für Bildung, Kultur und Wissenschaft im Rahmen seiner Verantwortung für den Datenschutz bei allen Schulen hinzuwirken hätte, müssten diese ihre Verarbeitung personenbezogener Daten überprüfen, ob sie den gesetzlichen Anforderungen aus dem SDSG und den Regelungen der Verordnung entspricht. Dabei geht es nicht allein um den Einsatz spezieller Schulverwaltungs- und Unterrichtsprogramme, sondern auch um die Verarbeitung personenbezogener Daten mit Office-Software (z. B. Word, Excel, Access) und bei Nutzung des Internet. Die Erforderlichkeit personenbezogener Angaben gerade in solchen eigenen Angeboten muss kritisch geprüft werden.

Dem Verwaltungspersonal der Schulen, vor allem aber auch Lehrern und Schülern muss ausreichendes Problembewusstsein bei der Verarbeitung personenbezogener Daten und die Kenntnis geeigneter Maßnahmen vermittelt werden, Gefahren auszuschließen oder zumindest zu begrenzen; verwiesen sei auch hier insbesondere auf die Risiken der Internet-Nutzung (u. a. fehlende Vertraulichkeit der Kommunikation, unsichere Integrität von eMails, Virenrisiko, Verknüpfung und Weiterverarbeitung beliebiger Inhalte, Erfassung von Zugriffsdaten bis hin zur Bildung von Persönlichkeitsprofilen).

Sinnvoll sind Hilfen bei der datenschutzgerechten Gestaltung von Angeboten (möglichst ohne Personenbezug, also ohne Lehrer-, Schüler- oder Elternlisten, ohne aktive Inhalte, ohne Cookies, ohne Gästebücher, Foren und Chats, keine Fotos oder privaten Adressen, Vermeidung von Webcams, kei-

ne kritischen Links), für den Datenschutz bei „elektronischen Visitenkarten“ der Schüler (keine privaten Angaben, keine Angaben über Verwandte, Freunde und Bekannte) und bei der Absicherung von eMails (z. B. durch Verschlüsselung; funktionale eMail-Adressen statt personenbezogener Adressen; auch im Rahmen eines Datenaustausches zwischen den Schulen untereinander und mit dem MBKW).

Zusammenfassend habe ich dem Ministerium folgende Anregungen vorgelegt:

- Information der Schulen über gesetzliche Anforderungen und daraus herrührende Konsequenzen (hierzu wäre unter anderem eine Bereitstellung der Gesetze, Verordnungen, Erlasse, Richtlinien, Vorschriften und Materialien auf dem Bildungsserver hilfreich)
- Überarbeitung der Verordnung vom 3.11.1986 unter Berücksichtigung der realen Situation im Schulalltag (z. B. private Datenverarbeitung der Lehrer), der technischen Weiterentwicklung (z. B. Vernetzung) und der aktuellen datenschutzrechtlichen Regelungen (z. B. keine Verpflichtung, sondern Unterrichtung zum Datenschutz)
- Integration des Datenschutzes, der Risiken und geeigneter Maßnahmen in die Aus- und Fortbildung der Lehrer und die Ausbildung der Schüler, insbesondere auch im Rahmen der Projekte „PC-Führerschein“ und „Lehren für die Zukunft“ und der Ausbildung der Lehramtsanwärter im Studienseminar
- Unterstützung der Schulen beim EDV-Einsatz durch geeignete Risikoanalysen und Sicherheitskonzepte gemäß der IT-Sicherheitsrichtlinie des Saarlandes und unter Berücksichtigung des IT-Grundschutzhandbuchs des BSI, Anforderungen an Vernetzung, Serverräume, Datensicherung (Dateisicherungen, Personalakten), IT-Revision und Datenschutzkontrolle, Funktionstrennung zwischen Administration und Kontrolle, Virenproblematik, geeignete Vernichtungsgeräte, Zugangskontrolle (insbesondere auch bei Hausmeister und Putzfrauen)
- Unterstützung der Schulen bei ihren Internet-Angeboten (z. B. Bereitstellung von Server-Space auf dem Bildungsserver bzw. evtl. Nutzung des kostenlosen Angebotes von T-Online für Homepages)
- Muster-Lösungen für Homepages, für Verträge mit Dienstleistern, Firewall-Absicherung von Netzen, Berücksichtigung der Anforderungen des LfD an Internet-Angebote, Vorlage von Zustimmungserklärungen, Verschlüsselung von eMails
- Betreuung der Schulen bei der Umsetzung der datenschutzrechtlichen Anforderungen (Beratung, Betreuung, Freigabe, Meldung zum Dateienregister, Dienstanweisung)

- Bereitstellung einheitlicher Schulverwaltungssoftware (z. B. Schüler- und Lehrerdaten, Stundenpläne) und Muster-Abwicklung für Freigabe und Meldung zum Dateienregister an einer ausgewählten Schule zur Übernahme der Unterlagen durch alle anderen Schulen
- Bereitstellung einheitlicher Software und Vermittlung günstiger Lizenzen (z. B. auch aus Landeslizenzen); Hinweise auf lizenzrechtliche Bestimmungen (z. B. Erforderlichkeit von Betriebssystem- und Softwarelizenzen für alle Computer und Netze, Kopieren nur im Rahmen der Verträge, besondere Regelungen bei Schullizenzen)
- Unterstützung der Schulen bei der Verarbeitung personenbezogener Daten und Umsetzung der gesetzlichen Anforderungen, Beteiligung des LfD, Freigabe, Meldung zum Dateienregister sowie beim EDV-Einsatz vor Ort (auch kompetente Betreuung der Informationstechnik)
- Einbringen der oben genannten Themen in Fachkonferenzen und Schulleiter-Dienstbesprechungen
- Überprüfung der Internet-Nutzung und des eMail-Betriebs im Ministeriums selbst und mit außerhalb gelegenen Stellen unter Berücksichtigung datenschutzrechtlicher Anforderungen (z. B. Verschlüsselung vertraulicher Daten)
- Bereitstellung ausreichend qualifizierten Personals an den Schulen und ausreichendem Zeitkontingent für die informationstechnische Betreuung
- Hinwirken auf ausreichende Mittelbereitstellung und Unterstützung durch die Schulträger.

14.2 Aushang von Klassenlisten mit Religionszugehörigkeit

Ein Petent beschwerte sich bei mir darüber, dass an der Schule seines Kindes außen an jedem Klassenzimmer eine Liste der Schüler der jeweiligen Klasse mit Angabe der Konfessionszugehörigkeit jedes Schülers ausgehängt war.

Zwar darf nach der Verordnung über die Erhebung, Verarbeitung und sonstige Nutzung personenbezogener Daten in den Schulen vom 3. November 1986 die Religionszugehörigkeit erfragt werden, weil sie etwa für die Teilnahme am Unterricht von Bedeutung ist. Es ist jedoch sicherzustellen, dass Unbefugte keinen Zugang zu personenbezogenen Daten der Schüler haben. Unbefugte in datenschutzrechtlichem Sinne sind alle Personen, die die Daten zu ihrer Aufgabenerfüllung nicht zur Kenntnis nehmen müssen. Auf den Schulbereich bezogen sind dies etwa Lehrpersonen, die in der jeweiligen Klasse nicht unterrichten, Hausmeister, Reinigungspersonal oder sonstige Besucher der Schule. Durch die Praxis der betroffenen Schule erhielt dieser Personenkreis Kenntnis von der Religionszugehörigkeit der einzelnen

Schüler, wodurch diese in ihren Persönlichkeitsrechten beeinträchtigt wurden.

Auf meine Intervention hin wurden die fraglichen Klassenlisten sofort abgehängt. Die Entschuldigung der Schulleitung, die Listen seien versehentlich ausgehängt worden, hat mich etwas überrascht und zeigt eine erstaunliche Unkenntnis bzw. Unsensibilität im Umgang mit personenbezogenen Daten.

14.3 PISA-Studie der OECD

Wie gut bereiten unsere Schulen ihre Schülerinnen und Schüler auf die Herausforderungen der Zukunft vor? Vermitteln sie das Wissen und die Fertigkeiten, die Wertvorstellungen und Haltungen, die Jugendliche brauchen, um als mündige Bürger aktiv und produktiv am gesellschaftlichen Leben teilnehmen zu können? So werden in einer Broschüre die Ziele der internationalen Schulleistungsstudie PISA der Organisation für wirtschaftlich Zusammenarbeit und Entwicklung beschrieben, an der sich neben 30 anderen Staaten auch die Bundesrepublik Deutschland beteiligt hat.

Zur Durchführung der Studie wurden die Leistungen von 15jährigen Schülerinnen und Schülern in den Bereichen Leseverständnis, Mathematik und Naturwissenschaften gemessen. Zusätzlich sollten die Schüler in einem Fragebogen Auskünfte zu folgenden Themen geben: Lese-, Schreib- und Fernsehgewohnheiten, Zugang zu Computern und elektronischen Medien, Freizeitinteressen, Einstellung zum Lesen und Lernen usw. Die Eltern sollten unter anderem Angaben machen zu ihrer Einschätzung der Schule sowie zu ihrem Beruf und ihrer Ausbildung.

Bei der datenschutzrechtlichen Beurteilung war von einer personenbezogenen Datenverarbeitung auszugehen, da, obwohl keine Namen erhoben wurden, eine Identifizierbarkeit einzelner Personen im Einzelfall nicht ausgeschlossen werden konnte.

Die Datenverarbeitung durfte deshalb nur stattfinden mit Einwilligung der betreffenden Eltern und Schüler. Nach entsprechender Intervention der Datenschutzbeauftragten der Länder wurden eine Einverständniserklärung formuliert und die Informationsschreiben für die Schüler und Eltern überarbeitet. Insbesondere gab es den Hinweis, dass die Teilnahme an der Studie freiwillig ist und dass die Einwilligung ohne Angabe von Gründen jederzeit widerrufen werden kann.

Konkretisiert wurden auch die thematischen Bereiche, die in den Schülerfragebogen angesprochen werden. Zusätzlich wurde das Angebot an die Eltern aufgenommen, die Schülerfragebögen im Sekretariat der Schule einsehen zu können.

Bemerkenswert ist, dass im Rahmen dieser Studie zunächst elementare datenschutzrechtliche Grundsätze nicht beachtet wurden. Ich gehe allerdings davon aus, dass die Beteiligten bei zukünftigen vergleichbaren Vorhaben die gewonnenen Erfahrungen im Sinne des Datenschutzes umsetzen werden.

15 Wirtschaft

15.1 Prüfung bei der Industrie- und Handelskammer

Im Berichtszeitraum wurde eine Querschnittsprüfung bei der Industrie- und Handelskammer (IHK) vorgenommen, bei der insbesondere Rechtsfragen zum Sachverständigenwesen bislang noch keine endgültige Klärung erfahren haben.

- Anonymisierung der Gutachten

  Die Kammer ist nach IHK-Gesetz und Gewerbeordnung berechtigt, Sachverständige zu bestellen und zu vereidigen. Diesen Rechtsgrundlagen entsprechend hat die Kammer eine Sachverständigenordnung erlassen, wonach der Bewerber zum Nachweis seiner besonderen Sachkunde von ihm erstattete Gutachten vorlegen kann.

  Wenn diese Gutachten aber den Auftraggeber erkennen lassen oder personenbezogene Daten von ihm oder sonstigen Dritten enthalten, erfährt die Kammer hiervon, ohne dass diese Daten im Zusammenhang mit der öffentlichen Bestellung der Sachverständigen von Bedeutung wären. Nach dem Erforderlichkeitsgrundsatz, wonach eine Datenübermittlung nur zulässig ist, wenn die personenbezogenen Daten vom Datenempfänger benötigt werden, dürfen solche Angaben deswegen im vorzulegenden Gutachten nicht enthalten sein. Weder die Sachverständigenordnung noch der Personalbogen zum Antrag auf öffentliche Bestellung und Vereidigung als Sachverständiger enthielten jedoch einen Hinweis auf die notwendige Anonymisierung; den habe ich gefordert.

  Der Einwand der IHK, es müsse auch die Richtigkeit der Gutachten durch Rücksprache mit den Auftraggebern festgestellt werden, überzeugt mich nicht. Jedenfalls bedarf es hierfür nicht der Datenweitergabe ohne Kenntnis der Betroffenen. Ich habe die IHK auf die mir zwischenzeitlich bekannt gewordene Auffassung des Bund-Länder-Ausschusses „Industrie- und Handelskammer“ hingewiesen, der Bewerber im Bestellungsverfahren müsse sich selbst um die Zustimmung des Gutachten-Auftraggebers bemühen, wenn das Gutachten in nicht anonymisierter Form vorgelegt werde. Die Kammer habe allerdings zu prüfen, ob die

anonymisierte Form nicht doch generell den Anforderungen im Bestellungsverfahren genüge.

Ich habe darum gebeten, die deutliche Aufforderung, zunächst nur anonymisierte Gutachten vorzulegen, auf den Unterlagen für die Sachverständigen-Bewerber anzubringen.

- Anzeigepflichten nach § 19 Sachverständigenordnung

  Ein weiterer Kritikpunkt betraf die den Sachverständigen auferlegte Pflicht, bei einem gegen sie gerichteten Strafverfahren, das ein Verbrechen oder Vergehen zum Gegenstand hat, selbst die Kammer hiervon zu unterrichten. In § 19 der als Satzung der IHK erlassenen Sachverständigenordnung ist eine solche Anzeigepflicht für den Sachverständigen vorgesehen. Mitgeteilt werden sollen der Erlass eines Haft- oder Unterbringungsbefehls, die Erhebung der öffentlichen Klage, der Termin zur Hauptverhandlung, das Urteil oder der sonstige Ausgang des Verfahrens.

  Die Bestimmung sehe ich in Widerspruch zu detailliert geregelten Mitteilungspflichten nach dem Justizmitteilungsgesetz. Zu dessen Ausführung bestimmt Nr. 24 der bundeseinheitlichen Anordnung über Mitteilungen in Strafsachen (MiStra), dass Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte befugt sind, in Strafsachen gegen öffentlich bestellte und vereidigte Sachverständige Mitteilungen an die Kammer zu richten. Dort ist auch die wesentliche Einschränkung enthalten, dass eine Mitteilung nur dann anzuordnen ist, wenn der Tatvorwurf auf eine Verletzung von Pflichten schließen lässt, die bei der Ausübung des Berufs zu beachten sind, oder er in anderer Weise geeignet ist, Zweifel an der Eignung, Zuverlässigkeit oder Befähigung hervorzurufen.

  Die in Nr. 4 MiStra aufgeführten Stellen (Gerichte, Staatsanwaltschaften, Vollstreckungsbehörden) prüfen insofern die Voraussetzungen im Hinblick auf die „Mitteilungswürdigkeit“ einer Verfahrensentscheidung an die IHK nach den angegebenen Voraussetzungen.

  Es liegt eine Umgehung dieser genau bestimmten Meldepflicht vor, wenn darüber hinaus dem Sachverständigen auferlegt wird, jedes Verbrechen oder Vergehen, das nicht von Amts wegen mitgeteilt wurde, im Wege der Selbstauskunft bei der IHK anzuzeigen. Die konkretisierenden Normen schützen den Sachverständigen vor der Offenbarung anhängiger Verfahren, die mit seiner Sachverständigentätigkeit nicht in Zusammenhang gebracht werden können. Sie enthalten außerdem nur bestimmte Verfahrensschritte, die mitzuteilen sind, wenn der Strafvorwurf sich verdichtet hat. Eine Mitteilung jeglichen gegen ihn gerichteten Strafvorwurfs kann ihm meines Erachtens nicht abverlangt werden.

Ich habe daher zum Schutze dieses Personenkreises vor übermäßiger Offenbarung persönlicher Angelegenheiten auch nach gegenteiliger Stellungnahme der IHK die Forderung aufrechterhalten, in der Sachverständigenordnung diese Bestimmung zu streichen.

- Nachschau nach § 20 Sachverständigenordnung

  Eine weitere Norm der Sachverständigenordnung schien mir nicht im Einklang zu stehen mit datenschutzrechtlichen Bestimmungen. Es geht hierbei um die Möglichkeit, dass von der Kammer beauftragte Personen zur Gefahrenabwehr nicht nur Geschäftsräume, sondern auch die Wohnung des Sachverständigen betreten können. Von datenschutzrechtlicher Bedeutung ist das deshalb, weil mit der möglichen Einschränkung der Unverletzlichkeit der Wohnung zugleich Eingriffe in das Recht auf informationelle Selbstbestimmung verbunden sind und Art. 13 Abs. 7 GG solche Befugnisse nur den Gefahrenabwehrbehörden zuerkennt, wozu die Kammer nicht zählt.

  Angesichts der zu § 17 Handwerksordnung ergangenen Rechtsprechung, die zu einer verfassungskonformen Modifizierung der Bestimmung geführt hat, sehe ich auch zu § 29 GewO zumindest eine verfassungskonforme Auslegung angezeigt. Diese schließt m. E. ein durch Satzung – ohne spezielle gesetzliche Grundlage hierfür – bestimmtes Betretungsrecht der Kammer zur Gefahrenabwehr neben den nach Polizeirecht den Polizeibehörden übertragenen Befugnissen aus; die entsprechenden Sätze in der Sachverständigenordnung sind zu streichen.

Die IHK hat nach ihren Angaben alle Rechtsfragen zur Sachverständigenordnung über den Deutschen Industrie- und Handelstag dem Bundesministerium für Wirtschaft vorgelegt, dessen Antwort noch aussteht. Eine abschließende Stellungnahme der IHK liegt zu dieser Frage daher ebenfalls noch nicht vor.

Die Behebung von mir gerügter Mängel im technisch-organisatorischen Bereich, die rechtzeitige Löschung der Daten in verschiedenen Bereichen, am Datenschutz orientierte Vertragsgestaltungen zur Auftragsdatenverarbeitung, Meldungen zum Dateienregister, die datenschutzgerechte Ausgestaltung der Formulare, und die Beachtung des Erfordernisses der Einwilligung bei ansonsten fehlender Rechtsgrundlage wurden hingegen durch die IHK in Aussicht gestellt.

15.2 Personenbezogene Daten der Wirtschaft im Internet

Im Rahmen der Überprüfung der IHK und der HWK sind auch Fragen an mich herangetragen worden, inwieweit von ihnen Daten der bei den Kammern registrierten Unternehmen im Internet veröffentlicht werden dürfen. Einerseits wird ein solcher „Service“ für die Unternehmen und mögliche Ge-

schäftspartner von manchen geradezu für selbstverständlich gehalten, andererseits ist nicht einsichtig, weshalb personenbezogene Daten Einzelner in diesem Zusammenhang geringeren Schutz genießen sollen.

Wie auch sonst muss für die Veröffentlichung die Einwilligung der Betroffenen oder eine gesetzliche Grundlage gegeben sein. In den Gesprächen habe ich stets verdeutlicht, dass für die weltweit abrufbaren Internet-Informationen - mit den gegenüber regionalen schriftlichen Veröffentlichungen gesteigerten Risiken für die informationelle Selbstbestimmung - bislang keine ausreichenden Rechtsgrundlagen zur Verfügung stehen.

Aus der Gewerbeordnung lässt sich zwar nicht aus dem Wortlaut, aber aus der Gesetzesbegründung das Recht auf eine Gruppenauskunft durch die Gewerbeämter herauslesen; nach meinem Verständnis darf diese aber nicht die vollständige Gruppe aller Gewerbetreibenden einer Region umfassen. Datenübermittlungsbestimmungen enthalten für Einzelübermittlungen zudem keine Befugnis, diese auch zu veröffentlichen. Voraussetzung einer Auskunft ist überdies ein berechtigtes Interesse hieran; dies ist für die Grunddaten und ihre Übermittlung, die in der Veröffentlichung liegt, an einen nicht bestimmbaren Personenkreis nicht überprüfbar. Für die Übermittlung weiterer Daten - über die Grunddaten (Name, betriebliche Anschrift, angezeigte Tätigkeit) hinaus - ist zudem ein rechtliches Interesse glaubhaft zu machen und es darf kein Grund zu der Annahme bestehen, dass die schutzwürdigen Interessen des Gewerbetreibenden überwiegen.

Für Handwerksbetriebe ergibt sich nach der Handwerksordnung ebenfalls eine vergleichbare Rechtslage.

Es kann daher nicht ausreichen, den Unternehmen lediglich eine Widerspruchsmöglichkeit für eine Aufnahme in eine "Betriebsdatenbank" im Internet einzuräumen. Datenschutzrechtlich kann solch eine Datenbank nur mit der Einwilligung auf eine sichere Grundlage gestellt werden. Über die Gefahren, die sich aus dem Medium "Internet" ergeben, ist bei der Einholung der Einwilligung noch ausdrücklich hinzuweisen.

In diesem Zusammenhang sollte auch nicht außer acht gelassen werden, dass die speichernden Stellen mit dem Einstellen der Daten in das Internet keinerlei Herrschaft mehr über sie haben, also weder Verfälschungen ausschließen noch sicherstellen können, dass die Daten korrigiert oder gelöscht werden.

15.3 Prüfung der Handwerkskammer

Im Berichtszeitraum wurde auch die Handwerkskammer (HWK) überprüft. Auch hier kristallisierten sich zentrale Themenbereiche heraus, denen von

Seiten der Handwerkskammer aus der Sicht des Datenschutzes zukünftig stärkere Beachtung beizumessen ist.

So erfolgte in der Vergangenheit die erforderliche Löschung von Daten nicht rechtzeitig. Für regelmäßige Datenübermittlungen war zu überprüfen, ob jeweils entsprechende Rechtsgrundlagen vorhanden sind. Die Vordrucke, mit denen Daten erhoben werden, sind ebenfalls teilweise umzugestalten, da Hinweise auf die einschlägigen Rechtsnormen fehlten.

Wenn Verträge mit anderen (öffentlichen oder privaten) Stellen zur externen Datenverarbeitung abgeschlossen werden, darf sich die Handwerkskammer nicht in der Rolle des unterlegenen Geschäftspartners fühlen, der sich den Bedingungen der Gegenseite gänzlich unterwerfen muss. Sie hat vielmehr darauf zu achten, dass sie ihrer Verantwortung als Auftraggeberin für die bei ihr gespeicherten Daten auch dann gerecht wird, wenn die Datenverarbeitung nicht im Hause stattfindet. Zur Gewährleistung der Datensicherheit beim Vertragspartner hat sie vertraglich Weisungen zu geben und sich selbst - auch bei öffentlichen Stellen - sowie dem Landesbeauftragten für Datenschutz bei nicht-öffentlichen Stellen ein Kontrollrecht im Vertrag einzuräumen. Nur unter diesen Kautelen läuft die Auftragsdatenverarbeitung ordnungsgemäß ab.

Auf einen Einzelpunkt meiner Prüfung möchte ich besonders eingehen:

In den Zuständigkeitsbereich der Handwerkskammer fällt insbesondere auch die Bekämpfung der Schwarzarbeit. Nach den im Jahre 1999 erlassenen Richtlinien zur Bekämpfung der Schwarzarbeit, die durch Gemeinsamen Erlass mehrerer Ministerien erstellt wurden, hat die Handwerkskammer - neben zahlreichen anderen öffentlichen Stellen und Institutionen - die Aufgabe, Schwarzarbeit in geeigneter Weise zu verhindern, zu erforschen und zu bekämpfen. Die Handwerkskammer hat zwar keine Zuständigkeit für die Verfolgung und Ahndung von Ordnungswidrigkeiten im Zusammenhang mit der Tätigkeit von Schwarzarbeitern. Zur Unterstützung der insofern zuständigen Behörden (Ordnungsämter der Gemeinden, Bußgeldbehörden der Landkreise) wurde jedoch ein Außendienstmitarbeiter vertraglich bestellt.

Die zu erforschenden Einzelfälle erhält dieser nach Weisung und im Auftrag der HWK, die ihrerseits wiederum auch von handwerklichen Fachverbänden zur Beauftragung ermächtigt wurde. Seine Berichte übergibt er der HWK, die mit den zuständigen Verfolgungsbehörden zusammenarbeitet.

Im Hinblick auf die Auskunftserteilung, bei der nach der Darstellung des Außendienstmitarbeiters auf die Freiwilligkeit hingewiesen wird, sieht die HWK den Außendienstmitarbeiter als Beauftragten der HWK nach § 17 Abs. 2 Handwerksordnung an. Die Befugnis zu Prüfungen und Besichtigungen, die in der Bestimmung auch enthalten ist, wurde ihm vertraglich nicht übertragen. Seine Tätigkeit ist vielmehr fast ausschließlich das Einholen von Aus-

künften in Verdachtsfällen. Es wurde jedoch nicht ausgeschlossen, dass er in Einzelfällen Fotos fertigt. Gebäudeaufnahmen können personenbeziehbare Daten beinhalten (§ 3 Abs. 1 SDSG). Jedenfalls mit Fotoaufnahmen von (identifizierbaren) Personen überschreitet der Außendienstmitarbeiter jedoch eindeutig seine Befugnisse, denn dies sind erkennungsdienstliche Maßnahmen, die nur den zuständigen Verfolgungsbehörden vorbehalten sind (vgl. § 81b StPO i.V.m. § 46 OWiG).

Bei einem Gespräch mit dem Außendienstmitarbeiter wurde schon auf die fehlende Befugnis zur Fertigung von Fotoaufnahmen hingewiesen. Ich gehe davon aus, dass zwischenzeitlich auch die damals fehlende förmliche Verpflichtung nach dem Verpflichtungsgesetz vorliegt, da die Handwerkskammer generell die Behebung der von mir gerügten Mängel zugesagt hat.

15.4 Übermittlung von Kontonummern an Private

Der nachfolgende Fall zeigt deutlich, wie unbefriedigend sich die Zweiteilung der Kontrollkompetenz für den Datenschutz im öffentlichen und nicht-öffentlichen Bereich auswirkt. Es ist für Petenten kaum nachvollziehbar, dass sie sich an zwei Stellen zur Klärung eines einheitlichen Lebenssachverhalts wenden müssen, wenn sie in ihm einen Datenschutzverstoß sehen. Beschwerden und Unverständnis über diese staatliche Regelung bleiben daher nicht aus.

Im konkreten Fall musste die Prüfung des Falles, der an mich herangetragen wurde, unterbrochen und in der Kompetenz des Ministeriums des Innern als Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich weiterverfolgt werden.

Es ging um die Datenverarbeitung einer Sparkasse, die als rechtsfähige Anstalt des öffentlichen Rechts in der Kontrollkompetenz des LfD steht. Ein Petent hatte Anlass daran zu zweifeln, dass die Sparkasse seine Kontodaten ausreichend geschützt hatte. Er hatte das Institut als Erbe mehrerer Konten - mit Erfolg - verklagt, weil es ihm ein Guthaben vorenthalten wollte. Mit Erstaunen stellte er, während der Prozess noch lief, fest, dass die Nummern der ererbten Konten auf einem gegen ihn als Schuldner und die Sparkasse als Drittschuldner gerichteten Pfändungs- und Überweisungsbeschluss auftauchten.

Auch mir gegenüber hat die Kasse in ihrer Stellungnahme beteuert, sie habe das Bankengeheimnis und damit auch den Datenschutz gewahrt. Dies schien mir insbesondere deshalb glaubhaft, weil nicht sie, sondern eine völlig andere Person den Pfändungs- und Überweisungsbeschluss gegen den Petenten erwirkt hatte. Auffallend war allerdings, dass in diesem Verfahren der Gläubiger von demselben Rechtsanwalt vertreten wurde, wie die Sparkasse im Prozess um die ererbten Guthaben. Zur Vervollständigung der

Prüfung hätte daher eine Nachfrage bei diesem Anwalt nahe gelegen. Denn aus meiner Sicht dürfte das Bankengeheimnis, sofern die „undichte“ Stelle im Rechtsanwaltsbüro zu finden gewesen wäre, in solchen Fällen nicht ins Leere laufen, weil die Daten nur im Rahmen des konkreten Mandats zweckgemäß verwandt werden und nicht für jedes beliebige andere Verfahren, in dem der Anwalt tätig wird, ebenfalls zur Verfügung stehen dürfen.

Hier endete jedoch meine Kontrollkompetenz, die es mir nicht erlaubte, eine etwaige Nutzung der Daten durch den Rechtsanwalt in Erfahrung zu bringen. Ich habe den Petenten an die Aufsichtsbehörde für den nichtöffentlichen Bereich beim Ministerium des Innern verweisen müssen.

Solche Fälle, die es auch in anderen Bereichen gibt, geben Anlass, bei der Novellierung des Saarländischen Datenschutzgesetzes darüber hinaus auch eine Zusammenlegung der Kontrollinstanzen in Erwägung zu ziehen.

16 Steuern

16.1 Prüfung der Steuerfahndungsstelle und der Bußgeld- und Strafsachenstelle

Sowohl bei der Steuerfahndungsstelle (Steufa) als auch bei der Bußgeld- und Strafsachenstelle (BuStra) zeigten sich Mängel in gleichen Themenbereichen.

16.1.1 Speicherungsdauer und Aufbewahrung von Unterlagen

Bei der Prüfung schienen mir zunächst die Aufbewahrungsfristen nicht konzeptionell festgelegt zu sein. In meiner Prüfungsmitteilung habe ich deshalb Vorschläge hierzu unterbreitet. Da die Beamten der Steuerfahndungsstelle den Hilfsbeamten der Staatsanwaltschaft, d.h. den Polizeibeamten, gleichgestellt sind, sehen sie Abstufungen bei der Aufbewahrung von Unterlagen vor, die denjenigen im Polizeibereich entsprechen.

Da der Verfahrensausgang, insbesondere bei Einstellung des Verfahrens, von erheblicher Bedeutung für die Zulässigkeit der weiteren Speicherung ist, muss die Steufa von der BuStra bzw. der Staatsanwaltschaft über den Ausgang des Verfahrens unterrichtet werden (Art. 32 Justizmitteilungsgesetz; Nr. 11 Anordnung über Mitteilungen in Strafsachen; § 407 Abs. 2 AO). In Abhängigkeit vom Ausgang eines Verfahrens sollen die Daten bei Steuerstraftaten und Steuerordnungswidrigkeiten generell gelöscht werden in Fällen

der Einstellung des Verfahrens nach § 170 Abs. 2 StPO,

der Einstellung wegen Todes,

des Freispruchs des Angeklagten.

Eine Einzelfallentscheidung ist zu treffen in Fällen

der Einstellung wegen Verfahrenshindernissen,

der Einstellung nach §§ 153, 153a, 153b StPO, § 398 AO

der Einstellung aus sonstigen Gründen.

Bei Steuerstraftaten, die danach noch gespeichert werden, sind Aufbewahrungszeiten bis zu maximal 10 Jahren zulässig. Jedoch müssen gestaffelte Zeiten festgelegt werden, die insbesondere die Schwere der Tat und die Wiederholungsgefahr berücksichtigen (analog § 38 Saarländisches Polizeigesetz).

Für Steuerordnungswidrigkeiten kommt eine Speicherung nur in Betracht, wenn die Ordnungswidrigkeit nicht den Bagatellbereich betrifft. In Abhängigkeit von der Höhe des Bußgeldes sind ebenfalls gestaffelte Aufbewahrungszeiten bis zu maximal 5 Jahren festzulegen.

Da Datenspeicherungen nur in dem einer Tat angemessenen Zeitraum zulässig sind, habe ich insbesondere in Fällen, in denen die Staatsanwaltschaft das Verfahren übernommen hat, darum gebeten, auf die Mitteilung der das Verfahren abschließenden Entscheidung (ggfls durch Nachfrage) hinzuwirken.

Nachdem mein Prüfbericht auch dem Finanzministerium als Aufsichtsbehörde vorlag, hat mir dieses zu meinem Erstaunen mitgeteilt, die Aufbewahrungsbestimmungen seien bundesweit mit den Ländern und dem Bundesministerium abgestimmt und durch Erlass des Finanzministeriums bereits im Jahre 1995 im Lande verbindlich in Kraft getreten. Hiervon hat die geprüfte Stelle mir nichts gesagt, sondern vielmehr den Eindruck erweckt, sie könne eigenständig Aufbewahrungsbestimmungen - wenn auch an gesetzlichen (Verjährungs-)Bestimmungen orientiert - festlegen.

Nach meiner Auffassung mangelt es aber den bundeseinheitlichen Aufbewahrungsbestimmungen an einer ausreichend sachgerechten Abstufung nach dem jeweiligen Ausgang des Verfahrens. In dem zuständigen Bund-Länder-Gremium sollte auch das Saarland sich für eine stärkere Abstufung der Fristen und frühzeitige Aussonderung der Unterlagen einsetzen.

16.1.2 Informationszentrale für den Steuerfahndungsdienst (IZ-Steufa)

Die Steuerfahndungsstellen der Bundesrepublik unterhalten eine Informationszentrale für den Steuerfahndungsdienst beim Finanzamt Wiesbaden (IZ-Steufa). Dorthin werden Fälle gemeldet, die nicht nur regionale Bedeutung

haben. Auch die Strafsachenstellen melden Fälle, bei denen eine überregionale Bedeutung zu vermuten ist.

Die Tätigkeit der IZ-Steufa beim Finanzamt Wiesbaden erfolgt als Auftragsdatenverarbeitung für die einzelnen Bundesländer. Das bedeutet, dass der Auftragnehmer (IZ-Steufa) personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers (Steufa und BuStra) verarbeiten darf (§ 5 Abs. 1 SDSG). Die Steufa und BuStra bleiben deshalb für die in Wiesbaden gespeicherten Daten, die von ihr gemeldet wurden, weiterhin verantwortlich.

Die IZ-Steufa darf die Daten auch nur solange speichern, wie sie zur Aufgabenerfüllung der meldenden Stelle erforderlich sind, und muss die Löschungsfristen entsprechend den Regelungen für die Aufbewahrung beachten.

Damit dies geschehen kann, ist es zwingend erforderlich, dass die gemeldeten Fälle registriert werden und die Gründe der Meldung (Überregionalität) in der jeweiligen Akte dokumentiert werden. Da dies bisher bei der Steufa nicht erfolgt war, ist sie nicht in der Lage, ihre Verantwortung als Auftraggeberin wahrzunehmen. Eine datenschutzrechtliche Überprüfung war deshalb ebenfalls nur eingeschränkt möglich, weil nur solche Fälle herangezogen werden konnten, an die sich der jeweilige Sachbearbeiter noch erinnerte.

Die Prüfung der vorgelegten Fälle gab aber in Einzelfällen Anlass zu Zweifeln, ob es sich hierbei wirklich um Fälle von überregionaler Bedeutung handelt.

Voraussetzung für die Annahme der Überregionalität ist die Bedeutung des Falles für mehrere Steuerfahndungsstellen. Durch die Meldung an die IZ-Steufa soll ja erreicht werden, dass Ermittlungen gegen denselben Täter nicht unabgestimmt nebeneinander herlaufen. Dies ist insbesondere der Fall, wenn der Steuerstraftäter sich durch ständigen Wechsel seines Wohnsitzes, seines Aufenthaltes oder seines Betätigungsortes seinen steuerlichen Verpflichtungen entziehen will. Weitere Voraussetzung ist, dass die Tat vorsätzlich begangen wurde; Fahrlässigkeitsdelikten kommt im Regelfall keine überregionale Bedeutung zu.

16.1.3 Automatisierte Verfahren

Der letzte Komplex betraf die automatisierten Verfahren, die ohne meine Beteiligung und ohne die erforderliche Meldung zum Dateienregister in Betrieb waren. Zudem war auf die Dienstanweisung für IT-unterstützte Arbeitsplätze bei den Finanzämtern hinzuweisen, hier insbesondere auf die Beachtung der mindestens 6-stelligen Länge von Passwörtern.

Obwohl die Stellungnahme des Finanzministeriums zu meinem Prüfbericht bereits zwei Jahre zurückliegt, sind die dargestellten Mängel noch nicht vollständig behoben. Die speichernde Stelle ließ sich aber wenigstens davon überzeugen, dass der konkrete Nachweis der überregionalen Bedeutung eines an die IZ-Steufa gemeldeten Falles gegenüber dem Landesbeauftragten für Datenschutz nicht durch die Berufung auf das Steuergeheimnis verwehrt werden darf.

16.2 Zulässigkeit einer Hundesteuerbestandsaufnahme durch private Unternehmen

Gerade im kommunalen Bereich wird überlegt, welche Aufgaben der öffentlichen Verwaltung rechtlich einer Privatisierung zugänglich und vor allem durch Private auch kostengünstiger zu erledigen sind. Dabei steht schon seit einigen Jahren die Hundebestandsaufnahme durch private Unternehmen zur Diskussion. Wie ich bei meinen Prüfungen feststellen konnte, haben einige Kommunen in der Vergangenheit von dem Angebot privater Firmen Gebrauch gemacht.

Ich habe stets darauf hingewiesen, dass ich dies aus folgenden rechtlichen Erwägungen heraus nicht für zulässig halte:

Auch die Hundesteuer unterliegt als kommunale Abgabe dem Steuergeheimnis nach § 30 Abgabenordnung (AO). Nach dem Kommunalabgabengesetz (KAG) besteht zwar die Möglichkeit, Stellen außerhalb der Verwaltung bestimmte Aufgaben zu übertragen (§ 12 Abs. 5 KAG). Die Gesetzesbegründung hebt jedoch hervor, dass dies nach den Vorschriften über den Datenschutz und unter Beachtung von Berufs- oder besonderen Amtsgeheimnissen (z.B. Steuergeheimnis, Sozialgeheimnis) zulässig sein muss. Als Verwaltungshilfe kommen insofern lediglich rein technisch-mechanische Tätigkeiten in Betracht. Um solche Tätigkeiten handelt es sich aber nicht, wenn etwaige Hundehalter und die sie umgebenden Personen von Privaten über die Haltereigenschaft in einem persönlichen Dialog, der meistens an der Haustür stattfindet, befragt werden. Mit Ermittlung der Hundehaltereigenschaft wird vielmehr die Steuererhebungsgrundlage bestimmt. Wenn in der Phase der Datenerhebung das Steuergeheimnis hier für eine spezielle Steuerart durchbrochen werden soll, bedarf dies meines Erachtens einer bereichsspezifischen Rechtsgrundlage im Steuerrecht. Eine solche Rechtsgrundlage fehlt indes sowohl im KAG als auch in der AO.

Ich habe sowohl die überprüften Kommunen als auch das private Unternehmen, das die Kommunen im Saarland für seine Tätigkeit umworben hat, über meine Rechtsauffassung informiert.

17 Statistik

17.1 Lehrer- und Unterrichtsstatistik

Für Planungs- und Verwaltungszwecke benötigt die Schulverwaltung zuverlässige Angaben über den Einsatz der Lehrkräfte, aus denen auch die künftige Entwicklung ableitbar ist. Wie bedeutsam derartige Aussagen über den engeren schulischen Bereich hinaus sind, belegen beispielsweise die periodischen Nöte, dem Bedarf entsprechend ausgebildete Lehrer zu finden. Nötig ist also eine geeignete statistische Datenbasis.

Für eine derartige Statistik, die in erheblichem Umfang personenbezogene Daten verarbeitet, gibt es derzeit keine ausreichende gesetzliche Grundlage. Nachdem das Statistische Landesamt mir mitgeteilt hatte, es beabsichtige eine partielle Lehrer- und Unterrichtserhebung zu Testzwecken auf freiwilliger Basis durchzuführen, habe ich deshalb bereits 1998 darauf hingewiesen, dass hierfür die Einwilligung aller Betroffenen einzuholen ist. Ein solches Verfahren habe ich aber bei Ausdehnung der Erhebung auf alle Schularten und einen größeren Teilnehmerkreis nicht nur für unpraktikabel gehalten, sondern ohne Schaffung einer spezialgesetzlichen Grundlage aus datenschutzrechtlicher Sicht auch für unzulässig, da im Schulordnungsgesetz für statistische Erhebungen der Erlass einer Rechtsverordnung vorgesehen ist.

Ohne eine solche Rechtsgrundlage dürfen nur Statistiken i.S.v. Geschäftsstatistiken erstellt werden, die mit bereits vorhandenen Daten zu erarbeiten sind. Personenbezogene Mitteilungen aus dieser Geschäftsstatistik dürfen den jeweiligen Geschäftsbereich (Schule oder Ministerium) jedoch nicht verlassen, weil sie ausschließlich der Aufgabenbewältigung der Ausgangsbehörde dienen (§ 9 SLStatG). Für die Unterrichts- und Lehrerbedarfsplanung hielt die oberste Landesbehörde jedoch eine eigene (Primär-)Statistik für erforderlich.

Insoweit konnte ich wohl Kultusministerium und Statistisches Landesamt von der Notwendigkeit einer Rechtsverordnung nach dem Schulordnungsgesetz überzeugen. Zu dem mir sodann vorgelegten Entwurf hierfür habe ich Hinweise und Anregungen gegeben sowie die Testerhebung an Gesamtschulen mit Hilfe einer speziell entwickelten Software technisch-organisatorisch begleitet.

Da aber eine Rechtsverordnung nach Ablauf von nunmehr über zwei Jahren bislang immer noch nicht ergangen ist, ist ihr Erlass dringend anzumahnen, sofern das Projekt wie geplant fortgeführt wird.

17.2 Mehrfache Heranziehung zu Statistiken

Für die Auskunftspflichtigen sind Befragungen keine reine Freude, erst recht nicht, wenn sie mehrfach hiervon betroffen werden. So ist verständlich, dass wiederholt Gegenstand von Anfragen war, in welchen Zeiträumen einzelne Auskunftspflichtige von der Last statistischer Erhebungen durch das Statistische Amt zu befreien sind.

Obwohl bereits die den Fragebögen beigefügten Merkblätter auf die gesetzlichen Bestimmungen zum Erhebungszeitraum hinweisen, haben die Petenten beispielsweise beim Mikrozensus Verwunderung darüber geäußert, dass zu mehreren aufeinanderfolgenden Jahren von denselben Personen statistische Angaben zu machen sind. Über die Lästigkeit hinaus stellen sich diese Befragungen ja auch als Eingriff in das Recht auf informationelle Selbstbestimmung dar, bei Wirtschaftsstatistiken jedenfalls dann, wenn es sich bei dem Unternehmen um einen Einzelkaufmann handelt.

Die Heranziehung erfolgt selbstverständlich nicht willkürlich oder aus Bosheit, sondern nach festgelegten Auswahlverfahren. Zur Statistik im Handel und Gastgewerbe habe ich in einem Einzelfall darauf hingewiesen, dass das dort angewandte mathematisch-statistische Auswahlverfahren zwar einen systematischen Austausch der jeweils Auskunftspflichtigen in größeren Zeitabständen vorsieht, dies allerdings nur unter der Einschränkung der stichprobenmethodischen Vertretbarkeit. Da die Größenordnung des Umsatzes die Statistik entscheidend mitbeeinflusst, kann es hier eine Schicht von Unternehmen mit den höchsten Umsätzen der jeweiligen Branche geben, für die sich die Wahrscheinlichkeit für eine Rotation oder einen Austausch gegen ein anderes Unternehmen gegen Null nähert.

Wenn eine derartige Fallgestaltung einen Einzelkaufmann trifft, wird die Belastung seines Rechts auf informationelle Selbstbestimmung, solange er sehr hohe Umsätze tätigt, unter Umständen zeitlebens fortbestehen.

18 Öffentlicher Dienst

18.1 Personaldatenverarbeitung im Ministerium für Inneres und Sport

Man erwartet, dass die Verarbeitung von Personaldaten in einem Ressort, das für das Datenschutzrecht und speziell auch für das Personalaktenrecht federführend ist, mustergültig ist. Eine Datenschutzprüfung im Personalreferat des Ministeriums für Inneres und Sport hat allerdings gezeigt, dass auch dort ähnliche Versäumnisse wie in anderen Dienststellen anzutreffen sind (vgl. 17. TB Nr. 14.3):

- Die in § 108f SBG festgelegten Fristen für die Aufbewahrung und Vernichtung von Personalunterlagen wurden nicht eingehalten. So waren

noch Personalakten von Beschäftigten vorhanden, die vor über 50 Jahren ausgeschieden waren; sie hätten längst ausgesondert oder dem Landesarchiv übergeben werden müssen. Auch gab es noch alte Bewerberdaten; diese sind nach § 29 Abs. 3 SDSG unverzüglich zu löschen, sobald feststeht, dass ein Dienst- oder Arbeitsverhältnis nicht zustande kommt und der Betroffene in eine weitere Speicherung nicht eingewilligt hat. Unterlagen, die bei der Bewerberauswahl angefallen sind (Bewerberübersicht, Interviewbogen des Vorstellungsgesprächs u. dergl.), sind spätestens dann auszusondern, wenn mit Einwendungen gegen das Auswahlverfahren nicht mehr zu rechnen ist.

- In den Personalakten fehlte das in § 108 Abs. 2 SBG vorgeschriebene vollständige Verzeichnis aller Teil- und Nebenakten. Betroffene können daher bei der Wahrnehmung ihres Einsichtsrechts nicht erkennen, bei welchen sonstigen Stellen noch weitere Vorgänge über sie angelegt sind.
- Von mir stichprobenweise eingesehene Personalakten enthielten auch Angaben über Dritte (Kollegen, Mitbewerber), z. B. in Übersichten über anstehende Dienstjubiläen, Bewerberlisten.

Das Ministerium hat zugesichert, die Mängel Zug um Zug auszuräumen.

Außerdem wurde festgestellt, dass Telefondaten der Mitarbeiter (Dienst- und Privatgespräche) über die in den Fernsprechrichtlinien festgelegten, mit der Personalvertretung und dem LfD abgestimmten Fristen hinaus in Listen oder auf Disketten gespeichert wurden. Die Daten wurden mittlerweile gelöscht.

Ein besonderes Problem stellt die derzeitige organisatorische Einordnung des Sachgebiets Heilfürsorge in das Personalreferat dar. Wird ein Beamter durch einen Dienstunfall verletzt, so wird ihm und seinen Hinterbliebenen Unfallfürsorge gewährt (§ 30 Abs. 1 Beamtenversorgungsgesetz). Die Unfallfürsorge umfasst unter anderem das Heilverfahren mit der notwendigen ärztlichen Behandlung, der Versorgung mit Arznei-, Heil- und Hilfsmitteln sowie Krankenhausbehandlung und Kuren. Dem Dienstherrn werden damit sensible medizinische Daten offenbart. Aus diesem Grunde hat der Gesetzgeber in § 108 a SBG für Heilfürsorge und Heilverfahren eine der Beihilfe (vgl. TZ 18.6) entsprechende Regelung getroffen. Sie sollen in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden.

Das Ministerium hat zugesagt, das Sachgebiet aus dem Personalreferat auszugliedern.

18.2 Information über Personalveränderungen per eMail

Das Personalreferat des Ministeriums für Bildung, Kultur und Wissenschaft hatte alle Mitarbeiter per eMail über Personalveränderungen informiert. Solche hausinternen Mitteilungen sind zwar sinnvoll und datenschutzrechtlich

auch zulässig, im internen Bereich auch ohne gesonderte Einwilligung der Bediensteten.

Die Übermittlung personenbezogener Daten ist jedoch auf den für die Zusammenarbeit der Beschäftigten notwendigen Umfang zu beschränken. Nicht erforderlich ist - wie hier geschehen - mitzuteilen, dass gekündigt wurde und welche Aufgaben außerhalb der eigenen Behörde künftig wahrgenommen werden.

18.3 Mitarbeiterbefragungen

Aufgrund der Erkenntnis, dass nur zufriedene Mitarbeiter gute Mitarbeiter sind, werden auch in der öffentlichen Verwaltung in zunehmendem Maße Mitarbeiterbefragungen durchgeführt.

Im Berichtszeitraum wurde eine solche Mitarbeiterbefragung bei der saarländischen Polizei durchgeführt. In Vorbereitung ist eine großangelegte Mitarbeiterbefragung bei fast sämtlichen Bediensteten der saarländischen Landesverwaltung. Bei beiden Projekten war bzw. ist meine Dienststelle beratend tätig.

Folgende Gesichtspunkte halte ich aus datenschutzrechtlicher Sicht für wesentlich:

- Die Teilnahme an der Befragung muss freiwillig sein. Die Mitarbeiter sind auf die Freiwilligkeit ausdrücklich hinzuweisen.
- Die Anonymität der die Fragebögen ausfüllenden Mitarbeiter muss gewährleistet sein.

  Sämtliche mir bisher bekannt gewordenen Mitarbeiterbefragungen sind von vornherein als anonyme Erhebungen konzipiert. In der praktischen Umsetzung kommt es darauf an, dass diese den Mitarbeitern garantierte Anonymität auch tatsächlich gewährleistet ist. Zu Problemen kann es hier kommen, wenn in den Fragebögen, was der Regelfall ist, statistische Angaben verlangt werden, wie z. B. Alter, Geschlecht, Zugehörigkeit zu Organisationseinheiten usw. Hier ist jeweils sorgfältig zu prüfen, ob durch eine Verknüpfung dieser Angaben eine Reidentifikation einzelner Mitarbeiter möglich ist. Allerdings wird diese Problematik dann entschärft, wenn die Auswertung der Fragebögen durch ein externes Institut durchgeführt wird, welches nicht über das zu einer Reidentifikation erforderliche Zusatzwissen verfügt und auch nicht erhält. Dies war bzw. ist bei den erwähnten Mitarbeiterbefragungen der Fall.

  Als wesentlich betrachte ich in diesem Zusammenhang weiterhin, dass die ausgefüllten Fragebögen entweder von den Mitarbeitern direkt an das auswertende Institut geschickt werden, oder dass verschlossene Urnen aufgestellt werden, etwa bei der jeweiligen Personalvertretung.

Selbstverständlich ist, dass die Fragebögen nach Erfassung durch das auswertende Institut vernichtet werden.

- Bei Darstellung der Auswertungsergebnisse darf kein Rückschluss auf bestimmte Personen möglich sein.

  Diese Gefahr steigt, je kleiner die Größe der auszuwertenden Organisationseinheit ist und je mehr persönliche Merkmale in der Auswertung miteinander verknüpft werden.

- Besondere datenschutzrechtliche Probleme werfen anonymisierte Mitarbeiterbefragungen auf, die Werturteile über andere Bedienstete, z. B. über Vorgesetzte enthalten. Hier halte ich die Einwilligung der von der Befragung betroffenen Vorgesetzten für erforderlich, da eine andere Rechtsgrundlage für die Verarbeitung ihrer personenbezogener Daten nicht ersichtlich ist.

18.4 Inhalt einer ärztlichen Bescheinigung für die Arbeitszeitregelung

Einige Dienstvereinbarungen über die Einführung der flexiblen Arbeitszeit lassen für chronisch Kranke und Beschäftigte, die infolge einer akuten Erkrankung über einen längeren Zeitraum auf ambulante ärztliche Behandlung angewiesen sind, ausnahmsweise eine Anrechnung von Arztbesuchen auf die Arbeitszeit zu. Ein Mitarbeiter der Landesverwaltung hat mir mitgeteilt, dass sein Personalreferat von ihm für diesen Zweck ein ärztliches Attest mit der Art der Erkrankung und Diagnose verlange. Ich halte diese Forderung in diesem Zusammenhang nicht für berechtigt.

Der Dienstherr oder Arbeitgeber darf grundsätzlich keine Einzelangaben über den Gesundheitszustand erheben. Daher enthält auch die Arbeitsunfähigkeitsbescheinigung keine Diagnose. Aus dem gleichen Grunde sind Schwerbehinderte nicht verpflichtet, der Personalstelle den Bescheid des Versorgungsamtes, in dem die einzelnen Behinderungen mit Diagnosen aufgeführt sind, vorzulegen, sondern lediglich eine Kopie des Schwerbehindertenausweises. Es gehört nicht zu den Aufgaben einer Personalstelle, medizinische Befunde und Diagnosen zu bewerten.

In diesem Falle genügt die Information, dass, wie häufig und wie lange Arztbesuche medizinisch geboten sind; nicht nötig sind jedoch nähere Hinweise zur Diagnose. Wenn die Personalstelle danach bezweifelt, dass die in der Dienstvereinbarung genannten Voraussetzungen vorliegen, kann sie eine Begutachtung durch den Amtsarzt veranlassen. Der Amtsarzt kann - mit Einwilligung des Betroffenen - Auskünfte beim behandelnden Arzt einholen und der Dienststelle das Ergebnis der Begutachtung - ohne medizinische Details - mitteilen.

18.5 Personalnebenakten in den Schulämtern

Das Saarland hat die unteren Schulaufsichtsbehörden zum Jahresende 2000 abgeschafft und die Schulräte unmittelbar in das Ministerium für Bildung, Kultur und Wissenschaft eingegliedert. In den Schulämtern wurden bisher Personalnebenakten der Lehrkräfte geführt, die in den zugeordneten Schulen - insbesondere Grund-, Haupt, Sekundar-, Real- und Gesamtschulen - eingesetzt sind. Ich erfuhr, dass vorgesehen sei, die in den Schulämtern über Jahre und Jahrzehnte hinweg angesammelten Personalunterlagen unbesehen den nunmehr zuständigen Schulleitern zu übergeben.

Gerade weil in der Praxis häufig über den notwendigen Umfang hinaus und oft zu lange Unterlagen in den Personalnebenakten enthalten sind, hatten Lehrer Grund zur Befürchtung, dass Schulleiter von Vorgängen Kenntnis erhalten, die lange zurückliegen und die für die Ausübung von Aufsichtsfunktionen überhaupt nicht mehr relevant sind. Dass es zumal in kleinen Schulen vielfach enge Kontakte zwischen Schulleitern und Lehrkräften gibt, räumt diese Sorge keineswegs aus. Aus eigenen Prüfbesuchen weiß ich auch, dass in den Schulen meist nicht die Voraussetzungen gegeben sind, Personalunterlagen sicher aufzubewahren, weil verschließbare Schränke fehlen.

Ich habe das Ministerium auf die Regelungen des Personalaktenrechts im Saarländischen Beamtengesetz (SBG) hingewiesen. In Personalnebenakten werden Duplikate von Unterlagen gesammelt, die sich auch in der (im Ministerium geführten) Grundakte befinden. Sie dürfen nur solche Unterlagen enthalten, die vor Ort zur rechtmäßigen Aufgabenerfüllung erforderlich sind (§ 108 Abs. 2 SBG). Ich habe verlangt, dass die Personalnebenakten vor der Weitergabe an die Schulleiter auf den erforderlichen Umfang ausgedünnt werden. Es widerspricht jedem Datenschutzverständnis, zunächst die Vorgänge in ihrem aufgeblähten Umfang den Schulleitern zu übergeben und von diesen zu erwarten, dass diese daraus die für ihre Aufgabenerfüllung erforderlichen Daten herausfiltern. Dies dürfte erfahrungsgemäß dazu führen, dass die Schulleiter aus Zeitmangel oder aus anderen Gründen die übernommenen Personalunterlagen unverändert weiterführen.

Das Ministerium hat eingeräumt, dass die vor der Neuorganisation angelegten Personalnebenakten „zum Teil“ noch Unterlagen enthalten, die über den notwendigen Umfang hinausgehen. Es hat sich jedoch wegen des Arbeitsaufwandes außerstande gesehen, die Unterlagen vor der Weitergabe zu reduzieren.

18.6 Beihilfebearbeitung bei Gemeinden

Über 80 % der saarländischen Gemeinden und Gemeindeverbände lassen die Beihilfe, die den Beschäftigten im Krankheitsfall zu gewähren ist, von der

Ruhegehalts- und Zusatzversorgungskasse des Saarlandes berechnen. Die vom Gesetzgeber geforderte Trennung der Beihilfefestsetzung von der Personalsachbearbeitung (§ 108a SBG) ist damit gewährleistet. Meine Nachforschungen, wie das Problem bei den übrigen Kommunen gelöst wird, ergaben ein unterschiedliches Bild:

- Mehrere Städte und Gemeinden haben die Beihilfebearbeitung aus der Personalstelle herausgenommen und einer anderen Organisationseinheit, meist Hauptamt oder Hauptabteilung, übertragen. Sie erfüllen damit die gesetzlichen Anforderungen.
- In drei Kommunen ist die Abschottung aus meiner Sicht nicht ausreichend. Es genügt nicht, die Beihilfestelle formell als eigenständige Einheit zu deklarieren, aber den Beihilfesachbearbeiter noch mit Aufgaben der Personalsachbearbeitung wie Besoldungsfestsetzung zu betrauen.
- In weiteren vier Gemeinden ist bisher überhaupt noch keine Bereitschaft zu erkennen, der Gesetzesforderung zu entsprechen. Nalbach und Schwalbach lehnen es unter Hinweis auf die kommunale Selbstverwaltung und darauf, dass § 108a SBG „nur“ als Sollvorschrift konzipiert sei, rundweg ab, irgendwelche Konsequenzen aus der geänderten Gesetzeslage zu ziehen.

  Ein Bürgermeister teilte mit, in seiner kleinen Verwaltung kenne ohnehin jeder jeden seit Jahren, teils schon aus der Schulzeit. In einem solchen Umfeld seien gewisse Unsitten der „privaten Kommunikation“ weder mit guten Worten noch mit der „Keule des Gesetzes“ auszurotten. Wenn die Situation wirklich so ist, finde ich, dass diese es geradezu zwingend notwendig macht, den Beschäftigten die Möglichkeit zu geben, Arzt-, Krankenhaus- und Arzneimittelrechnungen einer externen Stelle vorzulegen und zu verhindern, dass sensible Krankheitsdaten - auch der Angehörigen - den Kollegen der eigenen Verwaltung offen zu legen sind.

18.7 Beihilfe bei psychotherapeutischer Behandlung

Bei der Zentralen Beihilfefestsetzungsstelle der Oberfinanzdirektion habe ich das Verfahren überprüft, mit dem die Beihilfefähigkeit für Psychotherapien anerkannt wird. Solche werden erst bewilligt, wenn ein externer Gutachter die medizinische Notwendigkeit der Behandlung bescheinigt hat. Schwerpunkt meiner Überprüfung war, ob im Zusammenhang mit dessen Einschaltung datenschutzrechtliche Verbesserungen erforderlich sind.

Der externe Gutachter erstellt sein Gutachten auf der Grundlage eines Berichtes des behandelnden Arztes und des sogenannten Konsilliarberichtes, in dem ein anderer Arzt eine somatische Erkrankung ausschließt.

Folgende Punkte halte ich für verbesserungsbedürftig:

- Neben anderen personenbezogenen Daten des Patienten wird dessen Name und Vorname an den Gutachter übermittelt. Das halte ich bei der Beauftragung des externen Gutachters nicht für erforderlich. Ein Beleg ist für mich die Praxis der gesetzlichen Krankenkassen, die dem externen Gutachter lediglich eine Chiffre übermitteln. Das Argument, der externe Gutachter müsse den Namen des Patienten kennen, um Kontakt mit dem behandelnden Arzt aufnehmen zu können, kann ich nicht akzeptieren. Sollte eine solche Kontaktaufnahme tatsächlich einmal erforderlich sein, halte ich es wegen der besonderen Sensibilität der in Rede stehenden Daten für angemessen, den Weg über die Beihilfefestsetzungsstelle zu nehmen und den damit verbundenen organisatorischen Mehraufwand in Kauf zu nehmen.
- Der Fachgutachter soll sich, insbesondere bei positivem Votum, zu der Frage äußern, ob und in welchem Umfang die Behandlung medizinisch notwendig ist. Bei einer stichprobenweisen Überprüfung von Akten wurde allerdings festgestellt, dass die Ausführungen der Gutachter oft über diese Aussagen hinausgehen.
- In der Schweigepflichtentbindungserklärung muss der Fachgutachter, der das Gutachten erstellen soll, namentlich benannt werden. Ich halte diese Information für einen wichtigen Bestandteil einer informierten Einwilligung. Nicht nachvollziehen kann ich vor allem das Argument, der Gutachter müsse gegenüber dem Patienten grundsätzlich anonym bleiben, um objektiv entscheiden zu können. Mit den aus dem Rechtsstaatsprinzip abzuleitenden Grundsatz der Offenheit des Verwaltungshandelns ist für mich eine Verfahrensweise nicht vereinbar, die dem Antragsteller die Kenntnis des Namens des Gutachters verwehrt. Auch in sonstigen Verwaltungsverfahren, in denen Gutachten erstattet werden, ist es üblich, dass der Betreffende den Namen des Gutachters kennt. In der gesetzlichen Unfallversicherung hat der Versicherte sogar das Recht, unter mehreren Gutachtern auszuwählen (§ 200 Abs. 2 SGB VII).

In Bezug auf die Löschung der Daten im automatisierten System habe ich festgestellt, dass die Daten der letzten 12 Beihilfeanträge - unabhängig vom Bearbeitungszeitpunkt - gespeichert bleiben; bei jedem Folgeantrag werden die Daten des ältesten Antrages überschrieben. Dieses Verfahren der Datenlöschung steht mit den datenschutzrechtlichen Vorschriften nicht in Einklang. Die Daten sind zu löschen, wenn sie zur Aufgabenerfüllung bei der Beihilfegewährung nicht mehr erforderlich sind. Ein Löschungskonzept abhängig von der Speicherkapazität kommt nicht in Betracht.

Auf diesen Gesichtspunkt hatte ich bereits bei Einführung des Verfahrens im Jahre 1992 hingewiesen (14. TB, TZ 8.3.2). Die OFD hatte daraufhin ein geändertes Löschkonzept erarbeitet, das sowohl datenschutzrechtlichen als auch wirtschaftlichen und ablauftechnischen Gesichtpunkten angemessen

Rechnung tragen sollte. Sehr überrascht war ich, dass dieses neue Löschkonzept nie in die Praxis umgesetzt worden ist.

Ich habe daher gefordert, umgehend Maßnahmen zu ergreifen, um eine den datenschutzrechtlichen Anforderungen entsprechende Löschung der Beihilfedaten zu gewährleisten.

18.8 Sicherheitsüberprüfungsgesetz

Das Ministerium für Inneres und Sport hat den Entwurf eines Gesetzes zur Regelung der Voraussetzungen und des Verfahrens von Sicherheitsüberprüfungen erstellt; er liegt inzwischen dem Landtag vor.

Bedienstete in der öffentlichen Verwaltung, die Umgang mit geheimhaltungsbedürftigen Tatsachen oder Erkenntnissen haben oder erhalten sollen, werden einer Sicherheitsüberprüfung unterzogen. Das Sicherheitsüberprüfungsgesetz regelt die Art und Weise der Durchführung der Überprüfung, die Rechte und Pflichten der Betroffenen, den Umgang mit den anfallenden personenbezogenen Daten und die Aktenführung bei den beteiligten Behörden. Geregelt sind auch die Kontrollbefugnisse des Landesbeauftragten für Datenschutz.

Bei hohem Geheimhaltungsgrad (geheim, streng geheim) der Aufgaben, mit denen der Betroffene befasst ist, führt das Landesamt für Verfassungsschutz tief in das Privatleben und die Intimsphäre eindringende Ermittlungen durch, die auch Ehegatten, Verlobte und Lebensgefährten einbeziehen. So befragt das Landesamt für Verfassungsschutz sogenannte Referenzpersonen, das sind Personen, die den Bediensten seit längerer Zeit kennen, unter anderem zu Anhaltspunkten für geistige oder seelische Störungen oder zu Alkohol-, Drogen- oder Tablettenmissbrauch. Das Ergebnis hält das Landesamt für Verfassungsschutz in einer Sicherheitsüberprüfungsakte fest.

Grundlage der Sicherheitsüberprüfung ist bisher eine "Richtlinie für die Sicherheitsüberprüfung von Bediensteten des Saarlandes, sowie der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts". Eine gesetzliche Grundlage für das Verfahren besteht im Saarland, anders als im Bund oder anderen Bundesländern, derzeit nicht. Weil es hier um nicht unerhebliche Eingriffe in den verfassungsrechtlich geschützten Bereich des informationellen Selbstbestimmungsrechtes geht, habe ich seit Jahren eine klare Gesetzesgrundlage gefordert. Insofern begrüße ich grundsätzlich den jetzt vorgelegten Gesetzentwurf und hoffe auf eine zügige Verabschiedung.

Ich habe in einer Vielzahl von Detailfragen datenschutzrechtliche Verbesserungen vorgeschlagen, wie etwa stärkere Trennung des Geheimschutzes von der Personalverwaltung, kürzere Löschungsfristen für Dateien und Ak-

ten beim Landesamt für Verfassungsschutz oder großzügigere Regelungen in bezug auf Auskunfts- und Einsichtsrechte des Bediensteten.

Kritisiert habe ich weiter die Einschränkung der Kontrollbefugnisse des Landesbeauftragten für Datenschutz:

- Wenn, was aus Sicherheitsgründen in Betracht kommt, gegenüber einem Betroffenen die Auskunft über gespeicherte Daten verweigert wird, soll auch mir keine Auskunft erteilt werden, wenn die zuständige Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Damit entstünde gerade in dem besonders sensiblen Fall der Auskunftsverweigerung aus Sicherheitsgründen ein nicht hinnehmbarer kontrollfreier Raum. Dem Betroffenen sollte die Möglichkeit zur Einschaltung des Landesbeauftragten für Datenschutz gegeben werden, der allein das datenschutzrechtlich korrekte Handeln der Verfassungsschutzbehörde oder des Geheimschutzbeauftragten überprüfen kann.
- Für nicht sachgerecht halte ich auch, dass dem LfD die Einsicht in die Sicherheitsakte und die Sicherheitsüberprüfungsakte nicht gewährt werden soll, wenn die betroffene Person widerspricht. Dies ist eine ebenso unangemessene Einschränkung meiner Kontrollrechte zulasten der Persönlichkeitsrechte anderer am Verfahren beteiligter Personen wie die Regelung, wonach personenbezogene Daten einer Person, der Vertraulichkeit zugesichert worden ist, auch mir gegenüber nicht offenbart werden müssen, denn damit verfügen die genannten Personen über die Überprüfbarkeit, auch wenn es um Daten Dritter geht.

Gefordert habe ich schließlich, den Landesbeauftragten für Datenschutz selbst von der Sicherheitsüberprüfung ebenso auszunehmen wie andere Amtsträger, bei denen die verfassungsrechtliche Funktion oder die Art ihrer Berufung es ausschließen, die Tätigkeit von einer Sicherheitsüberprüfung abhängig zu machen. Die in der Wahl durch das Parlament geforderte Vertrauensposition und die damit ausgedrückte Entsprechung für die "Ministerialfreiheit" seiner Tätigkeit ist so bedeutsam, dass die Durchführung einer Sicherheitsüberprüfung für seine Person keinerlei Relevanz für seine Ernennung haben könnte, die damit verbundene Datenverarbeitung mithin nicht erforderlich wäre.

Ich hoffe, dass im Laufe der parlamentarischen Beratungen noch Änderungen vorgenommen werden, die die Persönlichkeitsrechte der Betroffenen stärken.

18.9 Einheitliches Personalverwaltungssystem

Das Saarland beabsichtigt, im Jahre 2001 in den Ministerien und den nachgeordneten Dienststellen das automatisierte Personalverwaltungssystem

EPVS einzuführen, das von Baden-Württemberg entwickelt wurde und dort bereits in mehreren Landesbehörden im Einsatz ist. Bei den Beratungen in den für diesen Zweck gebildeten Gremien war ich beteiligt, sodass datenschutzrechtliche Überlegungen frühzeitig eingebracht werden konnten. Die Endfassungen des Benutzungskonzepts, des Datenschutzkonzepts und der IT-Dienstanweisung waren bei Redaktionsschluss für diesen Bericht noch nicht fertiggestellt. Eine abschließende datenschutzrechtliche Beurteilung war deshalb bislang nicht möglich.

18.10 Parlamentarische Anfragen zu Personalvorgängen

Nicht selten betreffen parlamentarische Anfragen Personalangelegenheiten von Bediensteten.

Im Berichtszeitraum wurde ich mehrfach von der Landesregierung um eine datenschutzrechtliche Stellungnahme gebeten, wie solche Anfragen zu behandeln sind. Es stellt sich die Frage nach dem Verhältnis zwischen dem Kontrollrecht des Parlaments und der entsprechenden Informationspflicht der Regierung zu den Persönlichkeitsrechten und insbesondere dem informationellen Selbstbestimmungsrecht der von einer parlamentarischen Anfrage betroffenen Bediensteten.

Ich habe mich zu der Problematik wie folgt geäußert:

„Mit der generell üblichen Veröffentlichung der Antwort auf parlamentarische Anfragen würden gegenüber der Allgemeinheit Einzelinformationen offenbart, die als Personalaktendaten einen besonderen Schutz seitens der Personalverwaltung beanspruchen.

Weder die Fürsorgepflicht des Dienstherrn für seine Mitarbeiter noch deren (verfassungsrechtlich verbürgtes) Recht auf informationelle Selbstbestimmung gilt allerdings als absolute Schranke gegenüber dem (ebenfalls verfassungsrechtlich gesicherten) Fragerecht des Parlaments, das als solches ebenfalls keinen unbedingten Vorrang genießt. Anzustreben ist vielmehr, beide Positionen – gegebenenfalls auch durch die Art der Beantwortung, bei der möglicherweise Einzelangaben durch die Bildung von Antwortgruppen zusammengefasst werden können – zu vereinbaren. Dabei gilt:

Je herausgehobener die Position ist, zu dessen/deren Inhaber/in personenbezogene Daten erfragt werden, desto stärker ist das Informations- und Kontrollinteresse des Parlaments bzw. der Allgemeinheit zu gewichten und muss dementsprechend das Recht des Bediensteten auf informationelle Selbstbestimmung zurücktreten. Umgekehrt sind personenbezogene Daten umso intensiver zu schützen, je mehr sie eher der eigentlichen Privatsphäre des/der Bediensteten zuzuordnen sind und je weniger sie maßgebliches

Kriterium sein können für die Rechtmäßigkeit des in der Anfrage angesprochenen Verhaltens der Landesregierung.“

In diesem Zusammenhang habe ich mich auch an den Präsidenten des Landtages des Saarlandes gewandt mit der Anregung, grundlegende Regeln für eine Behandlung der Anfragen im Landtag selbst in einer eigenständigen Ordnung aufzustellen. Sie greift die schon in meinem 16. Tätigkeitsbericht (TZ 6.4) gegebene Anregung auf, generell in einem Gesetz oder einer gleichwertig mit Außenwirkung ausgestatteten Regelung des Landtags verbindliche Regeln für die datenschutzgerechte parlamentarische Tätigkeit zu setzen, wie sie im übrigen in den gemeinsamen Empfehlungen für geboten gehalten werden, auf die sich die Landtagspräsidenten selbst schon am 9.Mai 1995 verständigt haben.

19 Medien

19.1 Landesrundfunkgesetz

Das Landesrundfunkgesetz wurde in den vergangenen Jahren mehrfach geändert, wobei jeweils andere als datenschutzrechtliche Themen im Vordergrund standen. Zu der bereits in meinem letzten Bericht (TZ 17.2) angeregten Anpassung des Rundfunk - Datenschutzrechts an die EG-Datenschutzrichtlinie, an die ich im Rahmen meiner Beteiligung am Gesetzgebungsverfahren jeweils erinnert habe, ist es dabei nicht gekommen.

Datenschutzrechtliche Bedeutung kommt vor allem den Sicherungen zu, auf die sich alle Bundesländer im Vierten Rundfunkänderungsstaatsvertrag verständigt haben, um etwa zu verhindern, dass Nutzungs- und Abrechnungsdaten bei der Inanspruchnahme neuartiger Verbreitungstechniken unzulässig verarbeitet werden. Detaillierte Regelungen und allgemeine Verpflichtungen auf Datensparsamkeit enthält der für private Veranstalter anwendbare Abschnitt dieses Staatsvertrags. Er wurde mit dem Zustimmungsgesetz landesrechtlich verbindlich gemacht; die Vorschriften überlagern die Bestimmungen des Landesrundfunkgesetzes, dessen Wortlaut hiervon teilweise abweicht. Von einer entsprechenden Anpassung dieses Gesetzes war - vor Inkrafttreten des Staatsvertrags zum 1. April 2000 - bei der Novellierung 1998 und auch bei letzten Änderung anlässlich des Fünften Rundfunkänderungsstaatsvertrags noch abgesehen worden. Zugleich mit der von der Landesregierung in Aussicht genommenen Novelle sollte der Veränderungsbedarf bezüglich des Saarländischen Rundfunks geprüft werden.

19.2 Datensparsamkeit bei der Rundfunkfinanzierung

Die Finanzierung des öffentlich-rechtlichen Rundfunks in Deutschland erfolgt in erster Linie durch Gebühren, deren Höhe die Landesparlamente auf der

Grundlage einer Übereinkunft der Ministerpräsidenten festlegen. In geringerem Umfang erfolgt sie durch Einnahmen aus Werbung, deren Umfang und zeitliche Platzierung begrenzt ist, und durch Sponsoring; weitere Finanzierungsformen haben kaum Bedeutung. Das so gewachsene Finanzierungssystem hat verfassungsgerichtliche Anerkennung gefunden. Gleichwohl sind Gebührenhöhe und Grenzen, aber auch die Ergänzung oder der Ersatz durch andere Möglichkeiten seit jeher Gegenstand öffentlicher Diskussion, nicht erst seit der Konkurrenz privater Rundfunkveranstalter.

Verstärkt wurden solche Überlegungen - sowohl in den politischen Gremien wie auch unter den Rundfunkanstalten selbst - vernehmlich im Vorfeld der Gebührenanhebung, die zum Jahresbeginn 2001 mit dem Fünften Rundfunkänderungsstaatsvertrag festgelegt worden ist. Anlass hierzu gab neben dem verständlichen Bestreben der im Wettbewerb stehenden öffentlich-rechtlichen Anstalten nach angemessener (verbesserter) Finanzausstattung das verbreitete Unverständnis in der Bevölkerung über eine etwaige Rundfunkgebührenpflicht von Internet-Anschlüssen, die der Gebührenstaatsvertrag lediglich zeitlich herausgeschoben hat; das Anknüpfen der Zahlungspflicht an die bloße Möglichkeit zum Rundfunkempfang auch bei multifunktionalen Geräten, die primär ganz anderen Zwecken dienen, erscheint zunehmend fragwürdig. Und schließlich äußern immer wieder Teilnehmer Unmut über das praktizierte Verfahren zur Bestimmung der Gebührenpflichtigen bzw. hiervon Befreiten und zum Einzug der geschuldeten Beiträge, das mit einem hohen Ausmaß von Datenverarbeitung verbunden ist:

Hält jemand ein Rundfunkempfangsgerät zum Empfang bereit, ist er nach den staatsvertraglichen Bestimmungen verpflichtet, dies den Rundfunkanstalten (bzw. der Gebühreneinzugszentrale in Köln, deren sich alle Anstalten bedienen) anzuzeigen. Nicht alle kommen dieser Verpflichtung nach oder versäumen bei Umzügen etc. die Ummeldung. Deshalb erlauben in den meisten Ländern die melderechtlichen Bestimmungen einen Abgleich mit dem Melderegister, aus dem der GEZ regelmäßig Daten übermittelt werden, und zwar zahlenmäßig weit überwiegend derjenigen, die ihre Zahlungsverpflichtungen erfüllt haben, für diese also eigentlich ohne Erfordernis. Auch wenn inzwischen die Zugriffe auf den jeweiligen Anstaltsbereich begrenzt sind, gibt es auf diese Weise faktisch für die gesamte Bundesrepublik an einheitlicher Stelle ein Melderegister, das nahezu alle erwachsenen Einwohner enthält. Die Anstalten beauftragen weiter spezielle Gebührenbeauftragte, die mit unterschiedlichen Mitteln noch nicht gemeldete Rundfunkteilnehmer dazu anhalten, ihrer Gebührenpflicht nachzukommen; entsprechende Maßnahmen stoßen verschiedentlich auf Kritik bei den Betroffenen, die sich deswegen auch an die - in den meisten Ländern insoweit unzuständigen - staatlichen Datenschutzbeauftragten wenden. Eine Vielzahl von Datenerhebungen und -übermittlungen erfordert schließlich das Verfahren zur Befrei-

ung von der Rundfunkgebührenpflicht, in das teilweise die Sozialämter der Gemeinden eingebunden sind.

Die Entscheidung über ein mögliches Ablösen der bisherigen Rundfunkfinanzierung muss die bestehenden verfassungsrechtlichen Bindungen des öffentlich-rechtlichen Rundfunks ebenso berücksichtigen wie die ihm gewährleistete Funktionsfähigkeit. Werden aber grundlegende Überlegungen zu einer Neuordnung der Rundfunkfinanzierung angestellt, dann sollte Ziel sein, dieser ein möglichst datensparsames Modell zugrunde zu legen. Zum anderen darf ein Festhalten an derzeitigen Begriffen mit Fortentwicklung der Technik nicht zu unangemessenen Ergebnissen führen. In diesem Sinn haben sich die Datenschutzbeauftragten von Bund und Ländern mit einer Entschließung vom 12./13.10.2000 (Anlage 23) an die Bundesländer gewandt.

19.3 Fernsehreportagen und Zeitungsberichte über behördliches Handeln

Nicht immer sind es Beschwerden und Eingaben, die uns mit dem Datenschutz bei öffentlichen Stellen befassen. So erhielt ich mehrere Anfragen von Medienmitarbeitern, die an möglichst anschaulichen Informationen über die Arbeit von Vollstreckungsbeamten oder Hilfsdiensten interessiert waren und deshalb diese bei ihrer Arbeit begleiten wollten, ob hiergegen Bedenken bestünden. Dass trotz der zunehmenden Verbreitung von „Reality-Shows“ im Fernsehen die fragenden Journalisten das Gespür behalten haben, wie problematisch die Berichterstattung über Einsätze von Polizei, Hilfsdiensten oder Vollstreckungsbeamten für die Privatheit von Betroffenen sein kann, die ja hiermit nicht rechnen müssen, beruhigt.

Allerdings sahen meine Gesprächspartner das Problem allein oder in erster Linie in der Veröffentlichung der Bilder und Informationen und meinten, dem mit ausgetauschten Namen und verfremdeten Bildern Rechnung tragen zu können. Ich musste sie aber darauf hinweisen, dass schon die „erste Stufe“, also die bloße Teilnahme an der Arbeit der Beamten, einer rechtfertigenden Grundlage bedarf, wenn hierbei personenbezogene Daten zur Kenntnis genommen werden können. Dies ist weniger ein rechtliches Problem der Medien als der jeweiligen öffentlichen Stellen, deren Arbeit begleitet werden soll. Die Informationen darüber, dass ein bestimmter Bürger beispielsweise in Kontakt tritt zu Polizeibeamten, Gerichtsvollziehern oder Sozialhilfeermittlern, unterliegt speziellen Geheimhaltungsvorschriften oder dem allgemeinen Amtsgeheimnis. Die presserechtlich verbürgte Informationspflicht, der staatliche Stellen unterliegen, reicht als Rechtfertigung hierfür nicht aus, auch nicht zusammen mit einer ausdrücklichen Erklärung der Journalisten, die Verschwiegenheit zu wahren.

Denn wenn öffentliche Stellen im geduldeten und bewussten Beisein Dritter tätig werden (etwa bei einer Vollstreckungsmaßnahme oder im Hilfeeinsatz)

und hierbei von ihren Befugnissen zur Datenerhebung Gebrauch machen, geben sie faktisch Informationen an eine dritte Person weiter, die hiermit nichts zu tun hat und bei der auch nicht – wie in einem Notfall, bei dem Dritte zufällig anwesend sind - das Mithören und Mitsehen unvermeidbar ist. Das ist nicht nur dann unzulässig, wenn die jeweiligen öffentlichen Stellen noch an besonders betonte Verschwiegenheitspflichten gebunden sind wie bei dem Umgang mit Steuerdaten oder Gesundheitsdaten oder Umständen, die dem Sozialdatenschutz unterliegen.

Ein vergleichbares Problem stellt sich auch bei Berichterstattung über Vorgänge, bei denen ein besonderes Öffentlichkeitsinteresse deshalb angenommen wird, weil hieran Amtsträger oder andere Personen beteiligt sind, die aufgrund ihrer politischen oder wirtschaftlichen Stellung hohe Aufmerksamkeit genießen. Zum Umfang der den sogenannten „absoluten und relativen Personen der Zeitgeschichte“ zugebilligten Persönlichkeitsrechte sind im Berichtszeitraum zahlreiche gerichtliche Entscheidungen ergangen, die sich nach einer Verletzung der Rechte vor allem mit dem angemessenen materiellen Ausgleich für diese Persönlichkeitsrechtsverletzungen auseinandergesetzt haben. Es versteht sich von selbst, dass ein Ausgleich in Form einer Geldentschädigung für den Verletzten nicht alle Auswirkungen einer Persönlichkeitsverletzung erfassen und bereinigen kann.

Aufgabe des Datenschutzes ist es, präventiv darauf hinzuwirken, dass öffentliche Stellen sich an der Verletzung von Persönlichkeitsrechten durch die Medien nicht noch „konstruktiv“ beteiligen. Dabei verkenne ich nicht das Spannungsverhältnis, das durch das Auskunftsbegehren der Presse entstehen kann. Wir hatten uns mit Meldungen zu befassen, bei denen Betroffene einen derartigen Eingriff in ihre Privatsphäre annehmen konnten. In mehreren Fällen waren Angaben über betroffene Amtsträger so detailliert, dass die Vermutung nahe lag, ausschließlich eine öffentliche Stelle könne Informationen weitergeben haben, weil diese nur ihr zugänglich waren. Die Berichterstattung über Amtsträger, die einer Straftat verdächtigt wurden, kann so leicht einer Vorverurteilung gleichkommen; im konkreten Fall war dies angesichts der Tatsache, dass die Verfahren eingestellt wurden, weil der Tatverdacht sich nicht erhärtet hatte, um so bedauerlicher.

Auch ausgelöst von Hinweisen meines Kollegen in Rheinland-Pfalz, die dieser an die dortigen Behörden und Medien gerichtet hat, habe ich im Landesbereich festzustellen versucht, ob der Problematik in bereits bestehenden Regeln über die Öffentlichkeitsarbeit Rechnung getragen wird. Leider haben nur einzelne Ressorts geantwortet; der Gesichtspunkt fand nirgends ausdrückliche Erwähnung, auch nicht für die Polizei, für deren Informationsarbeit aber immerhin eine Reihe von Erläuterungen existieren. Um so mehr freut es mich, dass in die Gemeinsame Geschäftsordnung für die Obersten

Landesbehörden eine klarstellende Regelung aufgenommen werden soll, wie ich sie bei meiner Beteiligung angeregt habe.

20 Sonstiges

20.1 Wahlordnungen der Ärztekammer, der Apothekerkammer und der Tierärztekammer

Nach den Vorschriften des neuen saarländischen Heilberufekammergesetzes sind die Ärztekammer, die Tierärztekammer sowie die Apothekerkammer des Saarlandes verpflichtet, das Verfahren zur Wahl der Vertreterversammlung in einer Wahlordnung zu regeln. Das Ministerium für Frauen, Arbeit, Gesundheit und Soziales, das als Aufsichtsbehörde die Wahlordnungen genehmigen muss, hat mich zu den jeweiligen Entwürfen um Stellungnahme gebeten.

Der Datenschutz spielt insofern eine Rolle, als im Rahmen des Wahlverfahrens personenbezogene Daten der Wahlberechtigten, der gewählten Mitglieder der Vertreterversammlung oder auch der Mitglieder des die Wahl vorbereitenden und durchführenden Wahlausschusses verarbeitet werden.

Folgende Probleme stellten sich in mehr oder weniger ähnlicher Form bei allen Entwürfen:

- Es war vorgesehen, dass die Sitzungen des Wahlausschusses öffentlich stattfinden. Hierzu habe ich mich kritisch geäußert, denn in diesen Sitzungen kann auch über die Wählbarkeit oder Wahlberechtigung einzelner Kammermitglieder gesprochen werden. In diesem Zusammenhang können sensible Angelegenheiten zur Sprache kommen, z. B. Vorstrafen von Kammermitgliedern. Ich habe daher vorgeschlagen, die Teilnahmeberechtigung auf Kammermitglieder zu beschränken.
- Bei Veröffentlichungen aus den verschiedenen Anlässen, z. B. Veröffentlichung der Mitglieder des Wahlausschusses, Nennung der Wahlberechtigten im Wählerverzeichnis oder Veröffentlichung der gewählten Mitglieder der Vertreterversammlung war meist vorgesehen, auch die Privatanschriften anzugeben. Ich habe die Erforderlichkeit dieses Datums in Zweifel gezogen und vorgeschlagen, lediglich die Dienststelle oder die Praxis- bzw. Apothekenanschrift anzugeben.
- Bezüglich der Befugnis zur Einsichtnahme in das Wählerverzeichnis halte ich eine Beschränkung für erforderlich. Nach meiner Auffassung ist es zur Wahrung der Rechte der Wähler im Stadium der Wahlvorbereitung und zur Transparenz des Wahlvorbereitungsverfahrens ausreichend, wenn jeder materiell Wahlberechtigte die Möglichkeit besitzt, seine eigene Eintragung oder Nichteintragung im Wählerverzeichnis nebst

den seine Person betreffenden Angaben zu überprüfen. Ein darüber hinausgehendes Recht zur Einsichtnahme zwecks allgemeiner Prüfung der Richtigkeit oder Unvollständigkeit des Wählerverzeichnisses sollte nur bei Glaubhaftmachung eines berechtigten Interesses zulässig sein, um eine Einsichtnahme zu Ausforschungszwecken zu verhindern.

- Bei den Bestimmungen über die Einsichtnahme in die Wahlakte nach der Wahl durch die Wahlberechtigten war darauf zu achten, dass durch die Einsichtnahme das Wahlgeheimnis nicht durchbrochen wird. So ließe sich z. B. bei einer Kenntnisnahme der Wahlbriefumschläge erkennen, wer gewählt hat, bzw. aus dem Nichtvorhandensein eines Wahlbriefumschlages, wer nicht gewählt hat. Korrekt war daher ein Passus in der Wahlordnung der Apothekerkammer, wonach von der Einsichtnahme das Wählerverzeichnis mit den Vermerken über die Stimmabgabe, die Wahlbriefe, die Wahlbriefumschläge und die ungültigen Stimmzettel ausgeschlossen sind.
- Bedenken habe ich schließlich geltend gemacht, wenn zu lange Aufbewahrungsfristen für die Wahlakten vorgesehen waren. Für angemessen erachte ich eine Regelung, wonach Wahlunterlagen mit personenbezogenem Inhalt im Regelfall 60 Tage nach Ablauf der Einspruchsfrist vernichtet werden.

20.2 Veröffentlichungen von Geburtstagen von Kammermitgliedern

Immer wieder wurde in der Vergangenheit von Berufsvertretungen die Frage an mich herangetragen, ob und unter welchen Voraussetzungen es zulässig ist, persönliche Daten ihrer Mitglieder (z.B. Geburtstage, Beendigung der Tätigkeit) in Fachzeitschriften oder Mitteilungsblättern zu veröffentlichen. So wollte im Berichtszeitraum die Apothekerkammer des Saarlandes meine Auffassungen zu der Frage wissen, ob die runden Geburtstage der Kammermitglieder in einer Fachzeitschrift für Apotheken veröffentlicht werden dürfen.

Für die Mitglieder der Ärztekammer, der Apothekerkammer und der Tierärztekammer des Saarlandes regelt das saarländische Heilberufekammergesetz die Voraussetzungen, unter denen personenbezogene Daten der Kammermitglieder an andere Personen oder Stellen übermittelt werden dürfen. Nach § 3 Abs. 2 Satz 2 dieses Gesetzes dürfen die Daten an andere Personen oder Stellen nur mitgeteilt werden, wenn der/die Betroffene eingewilligt hat, ein Gesetz die Übermittlung ausdrücklich erlaubt oder, soweit dies zur Wahrnehmung gesetzlich übertragener Aufgaben erforderlich ist, an die Fürsorgeeinrichtungen der Kammern, die Versorgungswerke und die Aufsichtsbehörde.

Ausgehend von dieser eindeutigen Rechtslage musste ich der Apothekerkammer des Saarlandes mitteilen, dass eine Veröffentlichung nur möglich

ist, wenn die betreffenden Personen vorher einwilligen. Die von der Apothekerkammer des Saarlandes zur Diskussion gestellte „Widerspruchslösung“, wonach eine Veröffentlichung erfolgen kann, wenn der Betroffene nicht ausdrücklich widerspricht, konnte ich deshalb nicht akzeptieren.

20.3 Videoübertragung der Gedenkstätte Goldene Bremm

Nahe der Grenze zu Frankreich – abseits der Innenstadt Saarbrücken – liegt die KZ-Gedenkstätte Neue Bremm. Um sie in das Bewusstsein der Bevölkerung zu rücken, planten Studenten der Kunsthochschule des Saarlandes, das ehemalige KZ-Gelände mit einer Videokamera aufzunehmen und diese Videoaufzeichnungen auf im Stadtzentrum von Saarbrücken platzierte Monitore live zu übertragen.

Würden mit diesen Aufnahmen personenbezogene Daten verarbeitet, hätte es hierfür einer gesetzliche Grundlage bedurft, die es nicht gab; eine Einwilligung einzuholen, wäre ja faktisch nicht möglich gewesen. Aus datenschutzrechtlicher Sicht musste deshalb sichergestellt sein, dass auf den Videobildern keine Personen oder etwa PKW-Kennzeichen erkennbar sind.

Folgende Bedingungen für eine datenschutzgerechte Umsetzung des Projekts habe ich für erforderlich gehalten:

- Eine Veränderung des Bildausschnitts durch Schwenken oder Zoomen muss technisch ausgeschlossen sein. Eingriffe zur Änderung dieses Zustandes sind nicht zulässig.
- Der Bildvordergrund wird durch ein überlegtes Textband unsichtbar gemacht und an der linken unteren Ecke durch eine überlegte Matte oder dergleichen so verfremdet, dass keine Personen auf dem Parkstreifen erkennbar werden.
- Das Bildsignal wird auf geschützten Leitungen zu den vorgesehen Monitorpositionen übermittelt. Eine Weiterleitung an andere, insbesondere öffentlich zugreifbare Stellen oder Netze findet nicht statt.
- Das Bildsignal dient ausschließlich der zeitgleichen Wiedergabe an den vorgesehen Monitorstandpunkten; jede Aufzeichnung – auch durch die Kommunikationsbetreiber – wird ausgeschlossen.

Das Projekt wurde umgesetzt, inzwischen aber beendet.

Für die weitere Diskussion um die Zulässigkeit der Nutzung der Videotechnik ist es indes als Beispiel interessant, wenn man – ohne technische Restriktionen – eine Verarbeitung personenbezogener Daten ermöglicht. Wird, wie in Aussicht genommen, die Verarbeitung zugelassen, soweit dies zur Erfüllung des Geschäftszwecks oder zur Aufgabenerfüllung erforderlich ist, hätten in einem derartigen Fall an der Erforderlichkeit berechtigte Zweifel

bestanden. Kommt die Technik im künstlerischen Bereich ohne Einwilligung dann gar nicht mehr in Betracht?

Die Datenschutzbeauftragten des Bundes und der Länder bemühen sich, parallel zum derzeit laufenden Gesetzgebungsverfahren zum Bundesdatenschutzgesetz, um konkretisierende Lösungen bei der Abwägung von Informationeller Selbstbestimmung und anderen Interessen.

21 Anlagen

Anlage 1 **Modernisierung des Datenschutzrechts jetzt - umfassende Novellierung des BDSG nicht aufschieben**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999

Die deutschen Datenschutzbeauftragten haben bereits früh gefordert, die Novellierung des BDSG zur Umsetzung der EG-Datenschutzrichtlinie zu einer gründlichen Modernisierung des veralteten deutschen Datenschutzrechts zu nutzen. Da die dreijährige Anpassungsfrist im Oktober 1998 verstrichen ist, besteht jetzt ein erheblicher Zeitdruck. Für die Neuregelung, die derzeit in der Bundesregierung und in Koalitionsgremien vorbereitet wird, ist daher ein "Zwei-Stufen-Konzept" vorgesehen. Einem ersten, in Kürze vorzulegenden Novellierungsgesetz soll zu einem späteren Zeitpunkt eine zweite Änderung folgen, die weitere Verbesserungen enthalten soll. Die Konferenz geht davon aus, dass das Zweistufenkonzept von dem festen politischen Willen getragen wird, die zweite Stufe nach Einbringung des ersten Gesetzentwurfes zügig in Angriff zu nehmen und noch in dieser Legislaturperiode abzuschließen. Auch der in dieser Stufe bestehende Handlungsbedarf duldet keinen Aufschub.

Die Konferenz begrüßt, dass jetzt mit Hochdruck an der BDSG-Novellierung gearbeitet wird und Verantwortliche in Regierung und Fraktionen zugesagt haben, die erste Stufe der Neuregelung werde sich nicht auf das von der Richtlinie geforderte Minimum beschränken. Sie unterstützt die Vorschläge, Regelungen zur Videoüberwachung, zu Chipkarten und zum Datenschutzaudit aufzunehmen. Gleiches gilt für die Übernahme der zukunftsweisenden Bestimmungen zur Datenvermeidung sowie zur anonymen bzw. pseudonymen Nutzung von Telediensten aus dem Multimediarecht. Diese sind wichtige und dringend notwendige Regelungen zur Modernisierung des Datenschutzrechts. Die Konferenz drückt daher ihre Erwartung darüber aus, dass diese Vorschriften in der ersten Stufe des Gesetzgebungsverfahrens zügig verabschiedet werden.

Zu den Punkten, die keinen Aufschub dulden, gehört auch die Verbesserung der Voraussetzungen für eine effektive Datenschutzkontrolle. Die völlig unabhängige Gestaltung der Kontrolle im nichtöffentlichen Bereich muss institutionell sichergestellt und durch eine sachgerechte finanzielle und personelle Ausstattung unterstützt werden. Gegenwärtig noch bestehende Einschränkungen der Kontrollkompetenzen im öffentlichen Bereich müssen abgebaut, den Aufsichtsbehörden müssen wirksamere Befugnisse an die Hand gegeben werden.

Zum Schutz der Bürgerinnen und Bürger sind bei massenhaften Datenerhebungen mit unkalkulierbaren Datenverarbeitungsrisiken oder ungeklärter Zweckbestimmung klare materielle Grenzen durch den Gesetzgeber zu ziehen.

Die bereichsspezifischen Gesetze, z. B. die Sicherheitsgesetze, dürfen nicht vom Bundesdatenschutzgesetz mit den dort zu erwartenden substantiellen Fortschritten für die Bürgerinnen und Bürger, wie beispielsweise einem verbesserten Auskunftsrecht, abgekoppelt werden.

Notwendig ist nach Auffassung der Konferenz, dass das Datenschutzrecht auch in Zukunft bürgerfreundlich und gut lesbar formuliert ist. Dies ist eine unverzichtbare Akzeptanzvoraussetzung für den Datenschutz bei Bürgern, Wirtschaft und Verwaltung.

Anlage 2 **Geplante erweiterte Speicherung von Verbindungsdaten in der Telekommunikation**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999

Die Bundesregierung und der Bundesrat werden demnächst über den Erlass der seit längerem überfälligen Rechtsverordnung zum Datenschutz in der Telekommunikation auf Grund des Telekommunikationsgesetzes zu entscheiden haben.

Im Gegensatz zur früheren analogen Vermittlungstechnik erzeugt und verarbeitet das digitalisierte Telekommunikationsnetz (ISDN-Netz) in großem Umfang personenbezogene Verbindungsdaten. Dies zwingt zu begrenzenden, am Grundsatz der Datensparsamkeit orientierten Regelungen, um das Fernmeldegeheimnis und das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation zu garantieren.

Die bisher geltende Telekommunikationsdienstunternehmen-Datenschutzverordnung von 1996 sieht vor, dass die Verbindungsdaten unter Kürzung der Zielrufnummer regelmäßig bis zu 80 Tagen nach Versendung der Rechnung gespeichert werden dürfen. Über diese Frist hinaus dürfen Verbin-

dungsdaten nur gespeichert bleiben, wenn Streit zwischen dem Telekommunikationsunternehmen und den Kunden über die Richtigkeit der Abrechnung entsteht.

Demgegenüber gibt es Überlegungen für eine neue Telekommunikations-Datenschutzverordnung, dass alle Verbindungsdaten in der Regel selbst bei unbestrittenen oder bezahlten Rechnungen zwei Jahre lang nach Ende der Verbindung gespeichert bleiben können. Da die Speicherungsfrist erst am Ende des Jahres beginnen soll, in dem die Verbindung stattfand, kann dies in Einzelfällen dazu führen, dass die Daten bis zu drei Jahre lang vorgehalten werden.

Hiergegen wenden sich die Datenschutzbeauftragten des Bundes und der Länder mit Entschiedenheit. Sie sehen darin einen unverhältnismäßigen Eingriff in das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation. Auch das Telekommunikationsgesetz hebt die Grundsätze der Verhältnismäßigkeit und der Zweckbindung ausdrücklich hervor. Personenbezogene Daten, die für Zwecke der Telekommunikation erhoben und verarbeitet werden, dürfen nur solange gespeichert bleiben, wie es zu diesen Zwecken erforderlich ist. Auch die vom Gesetz geforderte Höchstfrist für die Speicherung von Verbindungsdaten muß sich am Grundsatz der Datensparsamkeit orientieren, solange sich die Kundin und der Kunde nicht ausdrücklich für eine längere Speicherung entscheiden.

Die Dauer einer zivilrechtlichen Verjährungsfrist kann ebenfalls kein rechtfertigender Anlass für eine solche Datenspeicherung sein. Jedenfalls müssen die Daten unverzüglich gelöscht werden, wenn die Rechnung beglichen und unbestritten ist und damit der vertragliche Speicherzweck erledigt ist.

Da eine telekommunikations- oder zivilrechtlich bedingte Notwendigkeit für eine derart lange Speicherfrist der Verbindungsdaten somit nicht ersichtlich ist, würde sie eine unzulässige Datenspeicherung auf Vorrat zu unbestimmten Zwecken darstellen.

Diese Speicherung von Kommunikationsdaten wäre auch nicht mit der Überlegung zu rechtfertigen, dass diese Daten zum Zwecke eventueller künftiger Strafverfolgung benötigt werden könnten. Die mit einer solchen Speicherung verbundene vorsorgliche Überwachung unverdächtiger Bürgerinnen und Bürger wäre unzulässig.

Anlage 3 **Transparente Hard- und Software**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999

Die Datenschutzbeauftragten des Bundes und der Länder haben sich wiederholt für die Nutzung datenschutzfreundlicher Technologien eingesetzt.

Sie sehen jedoch mit Sorge die Entwicklung im Bereich der Informationstechnik, die zu neuen Industriestandards und Produkten führt, die für die Benutzerinnen und Benutzer kaum durchschaubar und selbst für Fachleute nur noch eingeschränkt revisionsfähig sind.

Beispielsweise sind seit kurzem mit dem Intel Pentium III-Prozessor bestückte PCs auf dem Markt, deren Prozessor bei der Herstellung mit einer eindeutigen Nummer (Processor Serial Number - PSN) versehen wurde. Intel sieht vor, das Auslesen der PSN durch die Nutzerinnen und Nutzer kontrollieren zu lassen. Die mittlerweile bekannt gewordenen Manipulationsmöglichkeiten der dafür erforderlichen Software machen deutlich, dass die Existenz einer solchen eindeutigen Kennung kaum kontrollierbare Nutzungsmöglichkeiten eröffnet, die dem Datenschutz diametral zuwider laufen.

Die durch den Intel Pentium III initiierte Debatte um eindeutige Kennungen brachte ans Tageslicht, dass Softwarehersteller Nutzern neuerer Office-Produkte ohne deren Wissen eindeutige Kennungen zuordnen. Diese Kennungen können in Dokumenten versteckt sein und bei der Nutzung des Internets von Softwareherstellern verdeckt abgefragt werden.

Werden Daten der Nutzerinnen und Nutzer übermittelt, ohne dass sie dies bemerken, kann deren missbräuchliche Verwendung die Anonymität der Anwender von Informationstechnik weiter aushöhlen. Den Erfordernissen des Datenschutzes wird aber nur dann ausreichend Rechnung getragen, wenn zum Schutz der Privatheit transparente und von den Nutzerinnen und Nutzern in eigener Verantwortung bedienbare Sicherheitsfunktionen zur Verfügung stehen.

Deshalb erwarten die Datenschutzbeauftragten des Bundes und der Länder von Herstellern von Informations- und Kommunikationstechnik, Hard- und Software so zu entwickeln und herzustellen, dass Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit von Sicherheitsvorkehrungen überzeugen können.

Den Anwendern moderner Technik empfehlen die Datenschutzbeauftragten, nur solche Produkte einzusetzen, welche auch eine Transparenz der Verfahrensabläufe gewährleisten.

Anlage 4 **Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation (ENFOPOL '98)**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999

Gegenwärtig berät der Rat der EU über den Entwurf einer Entschließung zur grenzüberschreitenden Überwachung der Telekommunikation und der Internet-Nutzung (ENFOPOL '98).

Die Konferenz der Datenschutzbeauftragten hält es für inakzeptabel, dass der entsprechende Entwurf bisher geheimgehalten und ohne Einbeziehung der Datenschutzbeauftragten beraten wird.

Sie fordert die Bundesregierung auf, der Schaffung gemeinsamer Standards zur grenzüberschreitenden Überwachung der Telekommunikation nur insoweit zuzustimmen, als damit nicht zusätzliche Eingriffe in das Grundrecht auf unbeobachtete Kommunikation und das Fernmeldegeheimnis verbunden sind und die Nutzung datenschutzfreundlicher Technologien (z. B. prepaid cards) nicht konterkariert wird.

Anlage 5 **Gesundheitsreform**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 25. Oktober 1999

Die Datenschutzbeauftragten von Bund und Ländern erklären zu dem Entwurf eines Gesetzes "Gesundheitsreform 2000":

Die Datenschutzbeauftragten haben großes Verständnis für die Bemühungen, die Kosten im Gesundheitswesen zu begrenzen und eine gute Versorgung der Patientinnen und Patienten sicherzustellen. Bei der Wahl der Mittel ist es aber Aufgabe des Gesetzgebers, beim Eingriff in das Recht auf informationelle Selbstbestimmung das Prinzip der Erforderlichkeit und der Verhältnismäßigkeit zu wahren.

Der Entwurf lässt jede Begründung vermissen, warum die bisherigen Kontrollmechanismen, die das Entstehen umfangreicher medizinischer Patientendatenbestände bei den Krankenkassen vermeiden, ungeeignet sein sollen, die Wirtschaftlichkeit und Qualität ärztlicher Leistungserbringung sicherzustellen.

Der Entwurf gibt das bisherige Konzept der Datenverarbeitung in der gesetzlichen Krankenversicherung auf. Insbesondere standen bisher aus dem ambulanten Bereich personenbezogene Abrechnungsdaten mit medizinischen Inhalten und Diagnosedaten den Krankenkassen nur ausnahmsweise zu Prüfzwecken zur Verfügung, künftig sollen diese Informationen den Krankenkassen dagegen generell versichertenbezogen übermittelt werden. Damit entstehen bei den gesetzlichen Krankenkassen vollständige personenbezogene medizinische Datenbestände der gesetzlich Versicherten mit der Möglichkeit, für jede einzelne Person umfassende Darstellungen ihres Ge-

sundheitszustandes zu bilden. Bei den Kassen entstehen gläserne Patientinnen und Patienten. Das Patientengeheimnis wird ausgehöhlt.

Die Datenschutzbeauftragten richten an den Gesetzgeber die dringende Bitte, die bisher versäumte eingehende Prüfung von Erforderlichkeit und Verhältnismäßigkeit der weiterreichenden Datenverarbeitungsbestimmungen nachzuholen. Der Bundesbeauftragte für den Datenschutz, mit dem der Entwurf entgegen anders lautenden Äußerungen von Regierungsvertretern in der Sache bisher in keiner Weise abgestimmt wurde, sowie die Datenschutzbeauftragten der Länder stehen hierfür zur Diskussion zur Verfügung.

Insbesondere klärungsbedürftig sind folgende Punkte:

Der Entwurf erweitert die Aufgaben der Krankenkassen auch auf eine steuernde und durch die Patientinnen und Patienten nicht geforderte Beratung über Gesundheitserhaltungsmaßnahmen und auf eine Prüfung der u. a. durch die Ärztinnen und Ärzte erbrachten Leistungen. Er sieht dafür umfangreiche Datenerhebungs- und -verarbeitungsbefugnisse vor.

Der Wortlaut des Entwurfes beschreibt diese Aufgabe allerdings nur vage. Er lässt nicht erkennen, was auf die Patientinnen und Patienten zukommt. Weder ist klar geregelt, wie weit die Beratung reichen darf, noch mit welchen Rechtsfolgen die oder der Einzelne rechnen muss. Es ist zu befürchten, dass diese Beratung dazu dienen wird, die Patientinnen und Patienten, Ärztinnen und Ärzte und die sonstigen Leistungserbringer zu kontrollieren und zu beeinflussen und dass hierdurch das Arzt-Patienten-Vertrauensverhältnis belastet wird.

Wegen der vagen Aufgabenbeschreibung sind auch die damit verbundenen Datenverarbeitungs- und -zusammenführungsbefugnisse in gleicher Weise unklar und verschwommen. Eine Präzisierung und Eingrenzung ist dringend erforderlich.

Der Entwurf sieht im Gegensatz zum bisherigen System vor, dass Abrechnungsdaten und Diagnosen aus der ambulanten ärztlichen Behandlung generell patientenbezogen an die Krankenkassen übermittelt werden. Dadurch entstehen bei den Kassen umfangreiche sensible Datenbestände, aus denen sich für jede einzelne Patientin und jeden einzelnen Patienten ein vollständiges Gesundheitsprofil erstellen lässt. Wegen der Verpflichtung, die Diagnosen nach dem international gültigen ICD-10-Schlüssel zu codieren, sind diese medizinischen Informationen z. B. im Bereich der Psychotherapie auch hochdifferenziert.

Die zur Begründung besonders angeführten Punkte "Unterrichtung der Versicherten über die in Anspruch genommenen Leistungen, Kontrolle der Einhaltung der zweijährigen Gewährleistungspflicht bei den Zahnärzten, Unterstützung der Versicherten bei Behandlungsfehlern" vermögen insoweit nicht

zu überzeugen. Bereits jetzt können die Versicherten über die beanspruchten Leistungen und deren Kosten informiert werden und von ihrer Krankenkasse auch im Übrigen Unterstützung erbitten, so dass keine Notwendigkeit für die Anlegung derart sensibler, umfangreicher und zentraler Datenbestände ersichtlich ist.

Der Eingriff in die Rechte der Patientinnen und Patienten steht damit in keinem Verhältnis zu den angegebenen Zwecken.

Die beabsichtigte Einführung von zentralen Datenannahme- und -verteilstellen, bei denen nicht einmal klar ist, in welcher Rechtsform (öffentlich oder privat) sie betrieben werden sollen, hat eine weitere, diesmal Krankenkassen übergreifende zentrale Sammlung medizinischer personenbezogener Patientendaten zur Folge. Wegen des hohen weiteren Gefährdungspotentials von derart umfassenden Datenbeständen müsste der Entwurf im Einzelnen begründen, warum eine konsequente Umsetzung der schon bisher möglichen Kontrollmechanismen nicht ausreicht.

Die angesprochenen Punkte stellen besonders gewichtige, aber keineswegs die einzigen Probleme dar. Zu nennen sind hier nur beispielsweise die Verlängerung der Speicherdauer von Patientendaten beim Medizinischen Dienst der Krankenversicherung (MDK) von 5 auf 10 Jahre, unzureichende Regelungen bei den Speicherfristen, bei Umfang, Zweckbindung und Freiwilligkeit der Datenerhebung beim Hausarztmodell, der integrierten Versorgung und den Bonus-Modellen sowie unzureichende Pseudonymisierung bei den Arbeitsgemeinschaften. Abzulehnen ist auch die völlig mangelhafte Zweckbindung der Daten bei den Krankenkassen.

Anlage 6 **Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung zu Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich am 09./10.03.1995 gefordert, dass insbesondere die Dauer der Aufbewahrung von Strafakten nach rechtskräftigem Abschluss eines Strafverfahrens, ihre Aussonderung und Vernichtung einer Regelung durch formelles, den Grundsätzen des Volkszählungsurteils entsprechendes Gesetz bedarf.

Mit Beschluss vom 16.08.1998 hat das Oberlandesgericht Frankfurt am Main festgestellt, dass der derzeitige Zustand zwar für eine Übergangsfrist noch hinzunehmen sei, dass die Schaffung einer gesetzlichen Grundlage für die Aufbewahrung von Akten jedoch nicht als nur mittelfristige Aufgaben-

stellung des Gesetzgebers betrachtet werden dürfe, sondern alsbald in Angriff zu nehmen sei. In gleicher Weise hat auch das OLG Hamm mit Beschluss von 17.09.1998 darauf hingewiesen, dass die Aufbewahrung von Strafakten einer gesetzlichen Grundlage bedarf. Auch der Entwurf des Strafverfahrensänderungsgesetzes 1999 enthält insoweit keine Regelung.

Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für dringend geboten, dass unverzüglich mit der Umsetzung dieser Aufgabe begonnen wird. Sie weisen ferner darauf hin, dass auch für die Aufbewahrung von Zivilakten und Akten im Bereich der freiwilligen Gerichtsbarkeit umgehend gesetzliche Regelungen zu schaffen sind, die die Dauer der Aufbewahrung auf das erforderliche Maß festlegen.

Anlage 7 **Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

Die Ausbreitung moderner Telekommunikationsnetze und die Fortentwicklung der Informationstechnologie erfolgen in großen Schritten. Dieser technische Fortschritt hat einerseits zu einer massenhaften Nutzung der neuen Möglichkeiten der Telekommunikation und damit zu einer grundlegenden Veränderung des Kommunikationsverhaltens der Bevölkerung geführt. Andererseits erhalten dadurch die herkömmlichen Befugnisse der Strafverfolgungsbehörden zur Überwachung des Fernmeldeverkehrs eine neue Dimension, weil aufgrund der weitreichenden Digitalisierung immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden.

Die bei der Telekommunikation anfallenden Daten können mit geringem Aufwand in großem Umfang kontrolliert und ausgewertet werden. Anhand von Verbindungsdaten lässt sich nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Bereits auf der Ebene der bloßen Verbindungsdaten können so Verhaltensprofile erstellt werden, die die Aussagekraft von Inhaltsdaten erreichen oder im Einzelfall sogar übertreffen. Eine staatliche Überwachung dieser Vorgänge greift daher tief in das Telekommunikationsgeheimnis der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse.

Die bisherige rechtliche Grundlage für den Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in § 12 des Fernmeldeanlagengesetzes (FAG) stammt noch aus einer Zeit, in der die analoge Vermittlungstechnik vorherrschte, nicht für jedes Gespräch personenbezogene Verbindungsdaten erzeugt wurden und die Telekommunikationsdienste in wesentlich geringe-

rem Maße als heute genutzt wurden. Die Vorschrift erlaubt auch Zugriffe auf Verbindungsdaten wegen unbedeutenden Straftaten, bei denen eine inhaltliche Überwachung der Telekommunikation unzulässig wäre. Unter Berücksichtigung der Digitaltechnik, der vollständigen Datenerfassung und der Möglichkeit zur Bildung von Verhaltensprofilen verstößt § 12 FAG daher gegen den Verhältnismäßigkeitsgrundsatz und ist somit nicht mehr geeignet, Eingriffe in das Telekommunikationsgeheimnis zu rechtfertigen.

In einem früheren Gesetzesentwurf war vorgesehen, den Zugriff auf Verbindungsdaten grundsätzlich auf nicht unerhebliche Straftaten zu beschränken. Beschlossen wurde aber lediglich die unveränderte Fortgeltung des § 12 FAG, zuletzt befristet bis zum 31.12.1999. Nunmehr wollen der Bundesrat und die Justizministerkonferenz die Befristung für die Weitergeltung dieser Vorschrift aufheben und es damit beim bisherigen, verfassungsrechtlich bedenklichen Rechtszustand belassen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen eine Verlängerung der Geltungsdauer des § 12 FAG und fordern statt dessen eine Neufassung der Eingriffsbefugnis unter Beachtung der grundrechtlichen Bindungen und Anforderungen, die sich aus dem von Art. 10 Grundgesetz geschützten Telekommunikationsgeheimnis ergeben.

Die gesetzliche Ermächtigung für den Zugriff auf Verbindungsdaten gehört sachlich in die Strafprozessordnung. Die gesetzlichen Zugriffsvoraussetzungen sollten in Abstimmung mit § 100 a StPO neu geregelt werden.

Anlage 8 **DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

In der Strafprozessordnung ist der Einsatz der DNA-Analyse zur vorbeugenden Verbrechensbekämpfung nur mit richterlicher Anordnung vorgesehen.

In einigen deutschen Ländern werden DNA-Analysen ohne richterliche Anordnung gestützt allein auf die Einwilligung der Betroffenen durchgeführt. Soweit die dabei erhobenen Daten zum Zweck der Identitätsfeststellung in künftigen Strafverfahren genutzt werden sollen, bedürfen DNA-Analysen nach der klaren gesetzlichen Regelung des DNA-Identitätsfeststellungsgesetzes jedoch einer richterlichen Anordnung. Der Richter oder die Richterin hat u. a. die Prognose zu treffen, ob Grund zur Annahme besteht, dass gegen Betroffene künftig erneut Strafverfahren wegen des Verdachts erheblicher Straftaten zu führen sind. Wenn nunmehr auch DNA-Analysen gespeichert und zum Zweck der zukünftigen Strafverfolgung genutzt werden dürfen, die auf freiwilliger Basis - also ohne richterliche Anordnung - erstellt

worden sind, und dies sogar durch die Errichtungsanordnung für die DNA-Analyse-Datei beim BKA festgeschrieben werden soll, werden damit die eindeutigen gesetzlichen Vorgaben des DNA-Identitätsfeststellungsgesetzes unterlaufen.

Die von Strafgefangenen erteilte Einwilligung zur Entnahme, Analyse und Speicherung kann keine Grundlage für einen derartigen Eingriff sein. Eine wirksame Einwilligung setzt voraus, dass sie frei von psychischem Zwang freiwillig erfolgt. Da Strafgefangene annehmen können, dass die Verweigerung der Einwilligung Auswirkungen z. B. auf die Gewährung von Vollzugslockerungen hat, kann hier von Freiwilligkeit keine Rede sein. Ausschlaggebend für die Beurteilung der Freiwilligkeit einer Einwilligung ist die subjektive Einschätzung des Betroffenen. Auch wenn im Einzelfall die Weigerung von Strafgefangenen, sich einer DNA-Analyse zu unterziehen, die Entscheidung über Vollzugslockerungen nicht beeinflusst, ist dennoch davon auszugehen, dass die Befürchtung, die Verweigerung habe negative Folgen, die freie Willensentscheidung beeinträchtigen.

Die Datenschutzbeauftragten des Bundes und der Länder halten deshalb die Praxis einiger Länder, DNA-Analysen - abweichend von den gesetzlich vorgesehenen Verfahren - systematisch auf der Grundlage von Einwilligungen durchzuführen, für eine Umgehung der gesetzlichen Reglung und damit für unzulässig. Die möglicherweise mit der Beantragung richterlicher Anordnungen verbundene Mehrarbeit ist im Interesse der Rechtmäßigkeit der Eingriffsmaßnahmen hinzunehmen. Die Datenschutzbeauftragten fordern daher, DNA-Analysen zum Zweck der Identitätsfeststellung für künftige Strafverfahren nur noch auf der Grundlage richterlicher Anordnungen durchzuführen.

Anlage 9 **Beschluss des Europäischen Rates zur Erarbeitung einer Charta der Grundrechte der Europäischen Union**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

Der Europäische Rat hat anlässlich seiner Zusammenkunft am 4. Juni 1999 in Köln die Ausarbeitung einer Charta der Grundrechte der Europäischen Union beschlossen. In dem Ratsbeschluss heißt es: "Im gegenwärtigen Entwicklungszustand der Union ist es erforderlich, eine Charta dieser Rechte zu erstellen, um die überragende Bedeutung der Grundrechte und ihre Tragweite für die Unionsbürger sichtbar zu verankern".

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen nachhaltig die Initiative des Europäischen Rates zur Ausarbeitung einer europäischen Grundrechtscharta. Sie fordern Bundesregierung, Bundestag und Bundesrat auf, sich für die Einfügung eines Grundrechts auf Daten-

schutz in den zu schaffenden Katalog europäischer Grundrechte und dessen Verankerung in den Verträgen der Europäischen Union einzusetzen. Damit würde der herausragenden Bedeutung des Datenschutzes in der Informationsgesellschaft Rechnung getragen.

Die europäische Datenschutzrichtlinie verpflichtet die Mitgliedstaaten zur Gewährleistung des Schutzes der Grundrechte und Grundfreiheiten und insbesondere des Schutzes der Privatsphäre (Art. 1 Abs.1). Die Datenschutzbeauftragten weisen darauf hin, dass einige europäische Länder ein Datenschutzgrundrecht in ihre Verfassung aufgenommen haben; in einigen anderen Ländern wurde ihm durch die Rechtsprechung Grundrechtsgeltung zuerkannt. In Deutschland wird das vom Bundesverfassungsgericht aus dem Persönlichkeitsrecht (Art. 2 Abs. 1 i.V. m. Art. 1 Abs.1 GG) abgeleitete Grundrecht auf Datenschutz als solches von zahlreichen Landesverfassungen ausdrücklich erwähnt.

Anlage 10 **Patientenschutz durch Pseudonymisierung**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

Im Gesundheitsausschuss des Deutschen Bundestages wird derzeit der vom Bundesministerium für Gesundheit vorgelegte Gesetzesentwurf zur Gesundheitsreform 2000 dahingehend geändert, dass die Krankenkassen künftig von den Leistungserbringern (z. B. Ärztinnen und Ärzte, Krankenhäuser, Apotheken) die Patientendaten nicht in personenbezogener, sondern in pseudonymisierter Form erhalten. Dieses neue Modell nimmt eine zentrale Forderung der Datenschutzbeauftragten auf, für die Verarbeitung von Patientendaten solche technischen Verfahren zu nutzen, die die Persönlichkeitsrechte der Betroffenen wahren und so die Entstehung des "gläsernen Patienten" verhindern.

Auch anhand von pseudonymisierten Daten können die Krankenkassen ihre Aufgaben der Prüfung der Richtigkeit der Abrechnungen sowie der Wirtschaftlichkeit und der Qualität der Leistungen erfüllen.

Die Konferenz unterstützt den Bundesbeauftragten für den Datenschutz dabei, dass in den Ausschussberatungen die Wirksamkeit der Pseudonymisierung, die gesetzliche Festlegung von Voraussetzungen für die Identifizierung der Versicherten zu bestimmten Zwecken und die Definition strikter Zweckbindung dieser Daten durchgesetzt werden.

Anlage 11 **Eckpunkte der deutschen Kryptopolitik- ein Schritt in die richtige Richtung**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

Das Brief-, Post- und Fernmeldegeheimnis zählt zu den traditionellen und wichtigsten Garantien einer freiheitlichen Verfassung. Artikel 10 Grundgesetz gewährleistet deshalb die freie Entfaltung der Persönlichkeit durch einen privaten, vor Dritten verborgenen Austausch von Nachrichten, Gedanken und Informationen. Deshalb darf nur in Ausnahmefällen im überwiegenden Allgemeininteresse auf gesetzlicher Grundlage in dieses Grundrecht eingegriffen werden.

Im Zuge der Privatisierung der Telekom hat der Staat sein Post- und Fernmeldemonopol verloren, so dass zum Grundrechtsschutz die bloße Abwehr unrechtmäßiger staatlicher Eingriffe nicht mehr genügt. Darüber hinaus bestehen die Möglichkeiten der staatlichen Datenschutzkontrolle in offenen Netzen nur in eingeschränktem Maße. Der Schutz personenbezogener Daten während der Verarbeitung und Übertragung ist häufig nicht ausreichend gewährleistet. Deshalb sind ergänzende staatliche Maßnahmen zum Schutz Aller gegen neugierige Dritte (z. B. Systembetreiber, Unternehmen mit wirtschaftlichen Interessen, Hacker und Hackerinnen, ausländische Geheimdienste) erforderlich.

Die Privatsphäre lässt sich jedoch nur mit Rechtsvorschriften nicht ausreichend schützen. Neben bestehenden Ge- und Verboten sind wirksame technische Vorkehrungen nötig. Systemdatenschutz und datenschutzfreundliche Technologien sind unverzichtbar. Den Bürgerinnen und Bürgern müssen effektive Instrumente zum Selbstschutz an die Hand gegeben werden. Der Datenverschlüsselung kommt deshalb in einem modernen Datenschutzkonzept eine herausragende Bedeutung zu.

Bislang musste befürchtet werden, dass auf Betreiben der staatlichen Sicherheitsbehörden in Deutschland das Recht auf Verschlüsselung eingeschränkt würde. Jetzt jedoch hat die Bundesregierung mit dem Eckpunktepapier vom 2. Juni 1999 die Diskussion auf eine völlig neue Basis gestellt. Richtigerweise wird darin die Kryptographie als "eine entscheidende Voraussetzung für den Datenschutz der Bürger" besonders hervorgehoben.

Die Position der Bundesregierung, die freie Verfügbarkeit von Verschlüsselungsprodukten nicht einschränken zu wollen, wird von den Datenschutzbeauftragten des Bundes und der Länder ausdrücklich begrüßt. Damit wurde ein erster wichtiger Schritt in die richtige Richtung getan, dem jedoch weitere folgen müssen. Der im Sinne des Artikels 10 des Grundgesetzes legitime und grundrechtlich geschützte Anspruch Aller auf unbeobachtete Telekommunikation und auf den Schutz ihrer personenbezogenen Daten sollte von

der Bundesregierung noch stärker unterstützt werden. Um der Bedeutung geschützter Telekommunikation unter den Bedingungen der Informationsgesellschaft gerecht zu werden, sind konkrete Maßnahmen notwendig. Vorrangig sind zu nennen:

- Aktive Förderung des Einsatzes von Verschlüsselungstechniken in der öffentlichen Verwaltung, bei Privatpersonen und in Wirtschaftsunternehmen,
- Erbringung von Serviceleistungen, die den Gebrauch von effektiven Verschlüsselungsprogrammen für jedermann erleichtern,
- Maßnahmen zum besonderen Schutz der Telekommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte und Ärztinnen, Anwälte und Anwältinnen, Psychologen und Psychologinnen),
- Unterstützung von Wirtschaftsunternehmen beim Schutz ihrer geschäftlichen Telekommunikation,
- Förderung einer neutralen Bewertung von Verschlüsselungsprodukten mit dem Ziel, den Verbrauchern Empfehlungen für ihren Gebrauch zu geben, Förderung der Entwicklung europäischer Verschlüsselungsprodukte mit offengelegten Algorithmen.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten die öffentlichen Stellen auf, mit gutem Beispiel voranzugehen. Sie sollten vorbehaltlos die technischen Möglichkeiten des Einsatzes kryptographischer Verfahren zum Schutz personenbezogener Daten prüfen und derartige Lösungen häufiger als bisher einsetzen. Künftig muss Kryptographie der Standard in der Informations- und Kommunikationstechnik werden, auf deren Einsatz nur dann verzichtet wird, wenn wichtige Gründe dagegen sprechen.

Hersteller von Produkten der Informations- und Telekommunikationstechnik werden aufgefordert, die guten Voraussetzungen zur Entwicklung von Verschlüsselungsprodukten in Deutschland zu nutzen, um sichere, leicht bedienbare und interoperable Produkte zu entwickeln und den Anwendern kostengünstig anzubieten. Die Datenschutzbeauftragten des Bundes und der Länder bieten hierfür ihre Kooperation an.

Anlage 12 **"Täter-Opfer-Ausgleich und Datenschutz"**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

Kernstück datenschutzrechtlicher Überlegungen zum Täter-Opfer-Ausgleich ist die Frage, ob Institutionen zur Durchführung des Ausgleichsverfahrens

umfassende Informationen insbesondere über Opfer von Straftaten erhalten dürfen, ohne dass diese davon Kenntnis erlangt und eingewilligt haben.

Darin wäre ein unverhältnismäßiger Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen zu sehen. Dies ist nach geltendem Recht unzulässig.

Der nunmehr vorliegende Gesetzentwurf der Bundesregierung (BR-Drs. 325/99 vom 28.05.1999) sieht in § 155 a Satz 3 StPO-Entwurf vor, dass nur der ausdrücklich geäußerte entgegenstehende Wille der oder des Verletzten dazu führt, dass keine Datenübermittlungen an Schlichtungsstellen erfolgen sollen. Das bedeutet, dass solche im Einzelfall gleichwohl möglich sind. Dies halten die Datenschutzbeauftragten nicht für ausreichend.

Der Bundesrat ist sogar dem Gesetzentwurf der Bundesregierung nicht gefolgt; er hat vielmehr angeregt, im Gesetz klarzustellen, dass es für solche Datenübermittlungen auf den Willen der Opfer nicht ankommen soll. Folgende Argumente werden dafür genannt: Eine vor der Einschaltung von Schlichtungsstellen durch die Justiz einzuholende Einwilligung führe dazu, dass das kriminalpolitisch wichtige Institut des "Täter-Opfer-Ausgleichs" nicht ausreichend genutzt werde. Erst die professionelle Tätigkeit der Schlichtungsstellen mit ihrem Selbstverständnis als "objektive Dritte mit dem Gebot der Unterstützung jeder Partei" könnte wirksame Überzeugungsarbeit leisten; nur dann könne der Rechtsfriede dauerhafter als bei herkömmlichen Verfahren sichergestellt werden, wenn durch die "fachlich geleitete Auseinandersetzung" der "am strafrechtlich relevanten Konflikt beteiligten Parteien im Idealfall Verständnis und wechselseitige Toleranz geweckt werden".

Dieser Argumentation widersprechen die Datenschutzbeauftragten entschieden: Die Achtung und wirksame Unterstützung der Opfer ist ein wesentliches Anliegen des Strafverfahrens. Rechtsfriede und Toleranz können nur verwirklicht werden, wenn die Strafverfolgungsbehörden bei Datenübermittlungen an Schlichtungsstellen (z. B. in der Rechtsform von Vereinen) den Willen und die Eigenverantwortung der Opfer uneingeschränkt respektieren. Auch die Sicht der Beschuldigten, ohne deren Mitwirkung der Täter-Opfer-Ausgleich nicht durchgeführt werden kann, sollte von den Strafverfolgungsbehörden dabei berücksichtigt werden. Die Konferenz der Datenschutzbeauftragten fordert deshalb, dass an der Voraussetzung der unzweifelhaften Einwilligung vor solchen Datenübermittlungen festgehalten wird.

Ferner sollte der Gesetzgeber festlegen, dass die Berichte der Schlichtungsstellen an Staatsanwaltschaft und Gericht nur für Zwecke der Rechtspflege verwendet werden dürfen. Das besondere Vertrauensverhältnis zwischen den Schlichtungsstellen und den am "Täter-Opfer-Ausgleich" Beteiligten muss gesetzlich geschützt werden.

Anlage 13 **Risiken und Grenzen der Videoüberwachung**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000

Immer häufiger werden Videokameras eingesetzt, die für Zwecke der Überwachung genutzt werden können. Ob auf Flughäfen, Bahnhöfen, in Ladenpassagen, Kaufhäusern oder Schalterhallen von Banken oder anderen der Öffentlichkeit zugänglichen Einrichtungen, überall müssen Bürgerinnen und Bürger damit rechnen, dass sie auf Schritt und Tritt offen oder heimlich von einer Videokamera aufgenommen werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht darin die Gefahr, dass diese Entwicklung zur einer Überwachungsinfrastruktur führt.

Mit der Videoüberwachung sind besondere Risiken für das Recht auf informationelle Selbstbestimmung verbunden. Weil eine Videokamera alle Personen erfasst, die in ihren Bereich kommen, werden von der Videoüberwachung unvermeidbar völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen betroffen. Erfassung, Aufzeichnung und Übertragung von Bildern sind für die Einzelnen in aller Regel nicht durchschaubar. Schon gar nicht können sie die durch die fortschreitende Technik geschaffenen Bearbeitungs- und Verwendungsmöglichkeiten abschätzen und überblicken. Die daraus resultierende Ungewissheit, ob und von wem sie beobachtet werden und zu welchen Zwecken dies geschieht, erzeugt einen latenten Anpassungsdruck. Dies beeinträchtigt nicht nur die grundrechtlich garantierten individuellen Entfaltungsmöglichkeiten, sondern auch das gesellschaftliche Klima in unserem freiheitlichen und demokratischen Gemeinwesen insgesamt. Alle Menschen haben das Grundrecht, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch Kameras aufgezeichnet wird.

Daher müssen

- eine strenge Zweckbindung,
- eine differenzierte Abstufung zwischen Übersichtsaufnahmen, dem gezielten Beobachten einzelner Personen, dem Aufzeichnen von Bilddaten und dem Zuordnen dieser Daten zu bestimmten Personen
- die deutliche Erkennbarkeit der Videoüberwachung für die betroffenen Personen,
- die Unterrichtung identifizierter Personen über die Verarbeitung ihrer Daten
- sowie die Löschung der Daten binnen kurzer Fristen

strikt sichergestellt werden.

Jede Einrichtung einer Videoüberwachung sollte der datenschutzrechtlichen Vorabkontrolle unterzogen werden. Das heimliche Beobachten und Auf-

zeichnen, die gezielte Überwachung bestimmter Personen sowie die Suche nach Personen mit bestimmten Verhaltensmustern müssen grundsätzlich verboten sein. Ausnahmen müssen im Strafprozessrecht und im Polizeirecht präzise geregelt werden. Videoüberwachung darf nicht großflächig oder flächendeckend installiert werden, selbst wenn jeder Einsatz für sich gesehen gerechtfertigt wäre. Auch ein zeitlich unbegrenzter Einsatz ohne regelmäßige Erforderlichkeitsprüfung ist abzulehnen. Der Schutz der Freiheitsrechte erfordert überdies, dass heimliches Aufzeichnen und unbefugte Weitergabe oder Verbreitung von Aufnahmen ebenso strafbewehrt sein müssen wie der Missbrauch video-technisch gewonnener - insbesondere biometrischer - Daten und deren Abgleiche.

Dies bedeutet:

1. Bei einer gesetzlichen Regelung der Videoüberwachung durch öffentliche Stellen dürfen Einschränkungen nur aufgrund einer klaren Rechtsgrundlage erfolgen, die dem Grundsatz der Verhältnismäßigkeit Rechnung trägt.

- Die Voraussetzungen einer Videoüberwachung und der mit ihr verfolgte Zweck müssen eindeutig bestimmt werden. *Dafür kommen - soweit nicht überwiegende schutzwürdige Belange von Betroffenen entgegenstehen - unter anderem in Betracht*
  - *die Beobachtung einzelner öffentlicher Straßen und Plätze oder anderer öffentlich zugänglicher Orte, auf denen wiederholt Straftaten begangen worden sind, solange tatsächliche Anhaltspunkte dafür bestehen, dass dort weitere Straftaten begangen werden (Kriminalitätsschwerpunkte) und mit der Beobachtung neben der Sicherung von Beweisen eine Präventionswirkung erreicht werden kann; der Grundsatz der Verhältnismäßigkeit ist dabei strikt zu beachten. Ungezielte Verlagerungsprozesse sollten vermieden werden.*
  - *für die Verkehrslenkung nur Übersichtsaufnahmen,*
  - *der Schutz öffentlicher Einrichtungen im Rahmen der ordnungsbehördlichen Gefahrenabwehr, solange eine besondere Gefahrenlage besteht[1].*
- Maßnahmen im Rahmen des Hausrechts dürfen den grundsätzlich unbeobachteten Besuch öffentlicher Gebäude nicht unverhältnismäßig einschränken.
- Die Videoüberwachung ist für die Betroffenen durch entsprechende Hinweise erkennbar zu machen.

[1] Kursiv gedruckter Text wurde bei Stimmenthaltung der LfD Brandenburg, Bremen, Mecklenburg-Vorpommern, Nordrhein-Westfalen angenommen

- Bildaufzeichnungen sind nur zulässig, wenn und solange sie zum Erreichen des verfolgten Zweckes unverzichtbar sind. Die Anlässe, aus denen eine Bildaufzeichnung ausnahmsweise zulässig sein soll, sind im einzelnen zu bezeichnen. Die Aufzeichnungen sind unverzüglich zu löschen, wenn sie hierzu nicht mehr erforderlich sind oder überwiegende schutzwürdige Belange von Betroffenen entgegenstehen.
- Werden die Aufnahmen einer bestimmten Person zugeordnet, ist diese zu benachrichtigen, sobald der Zweck der Speicherung dadurch nicht gefährdet wird.
- Zur Prüfung der Normeffizienz ist festzulegen, dass das jeweils zuständige Parlament jährlich über die angeordneten Maßnahmen, soweit sie mit einer Speicherung der erhobenen Daten verbunden sind, und die mit ihnen erreichten Ergebnisse unterrichtet wird.

Bei der Videoüberwachung muss in besonderer Weise den Grundsätzen der Datensparsamkeit und Datenvermeidung Rechnung getragen werden. Die Chancen, die die modernen Technologien für die Umsetzung dieser Grundsätze, insbesondere für die Reduzierung auf tatsächlich erforderliche Daten bieten, sind zu nutzen.

2. Der Gesetzgeber ist auch aufgefordert, für die Videoüberwachung durch Private Regelungen zu schaffen, die den für die optisch-elektronische Beobachtung durch öffentliche Stellen geltenden Grundsätzen entsprechen. Dabei muss sichergestellt werden, dass optisch-elektronische Systeme, die die Identifizierung einzelner Personen ermöglichen, nur zur Abwehr von Gefahren für Personen und zum Schutz gewichtiger privater Rechte eingesetzt werden dürfen. Die privatrechtlichen Regelungen zum Schutz des eigenen Bildes durch das Vertragsrecht, das Deliktsrecht, das Besitz- und Eigentumsrecht, das Kunsturheberrecht und die dazu ergangene Rechtsprechung reichen nicht aus.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet, dass die Gesetzgeber bei der Novellierung der Datenschutzgesetze und anderer Gesetze diese Grundsätze berücksichtigen.

Anlage 14 **Für eine freie Telekommunikation in der freien Gesellschaft**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000

Umfang und Intensität der Eingriffe in das von Art. 10 Grundgesetz geschützte Fernmeldegeheimnis haben in den letzten Jahren deutlich zugenommen. Ursächlich hierfür sind zum einen folgende Aspekte:

- Erhebliche Zunahme der Telekommunikationsvorgänge
  Die Zahl der Telekommunikationsvorgänge hat sich vervielfacht. Darüber hinaus werden neben dem traditionellen Telefon neue Kommunikationsmöglichkeiten wie Fax und PC-Fax, das Mobiltelefon, e-mail und mailboxen sowie das Internet genutzt.
- Stark angestiegener Umfang und wesentlich verbesserte Aussagequalität der Daten
  - Die digitale Datenverarbeitung ermöglicht detaillierte Auswertungen großer Datenmengen.
  - Die Datenverarbeitungsnetze bieten mehr und mehr aussagekräftige Bestandsdaten, wozu auch e-mail-Adresse, IP-Nummer oder domain name gehören. So können sich bei Mitgliedschaft in geschlossenen Netzen sogar Rückschlüsse auf Lebensanschauungen oder bestimmte Problemlagen ergeben, z. B. bei der Mitgliedschaft in bestimmten Interessengemeinschaften, etwa Aids-Selbsthilfegruppen.
  - Die Verbindungsdaten geben in der Regel Auskunft, wer wann mit wem wie lange und wie häufig kommuniziert hat; werden fremde Geräte verwendet, geraten Unbeteiligte in Verdacht.
  - Aus den Nutzungsdaten von Tele- und Mediendiensten lassen sich Rückschlüsse auf Interessengebiete und damit auf persönliche Eigenheiten und das Verhalten der Nutzenden ziehen.
  - Mobiltelefone ermöglichen schon im Stand-by-Modus die Bestimmung ihres Standorts.
- Erleichterte Kenntnisnahme und Weiterverarbeitung dieser Daten
  Die wesentlich erweiterten und einfacher nutzbaren technischen Möglichkeiten erlauben es, an verschiedenen Orten gespeicherte Daten zur Kenntnis zu nehmen und zu verarbeiten.
- Entwicklung des Internets zum Massenkommunikationsmittel
  Über das Netz werden immer mehr Alltagsgeschäfte abgewickelt: Wahrnehmung verschiedenartiger Informationsangebote, Erledigung von Bankgeschäften, Buchung von Reisen oder Bestellung von Waren und Dienstleistungen in virtuellen Kaufhäusern (e-commerce). Dadurch fallen immer mehr auswertbare Informationen über Lebensgewohnheiten und Bedürfnisse der Bürgerinnen und Bürger an.
- Schwer durchschaubare Rechtslage

  Die Zersplitterung der Regelungen in Strafprozess-, Telekommunikations- und Multimediarecht machen diese wenig transparent und schwer anwendbar.

Zum anderen ist dieser größere, leichter auswert- und verarbeitbare Datenpool wachsenden Zugriffswünschen der Sicherheitsbehörden im weitesten Sinn auf nationaler und internationaler Ebene ausgesetzt:

- Die Zahlen der Telekommunikations-Überwachungsanordnungen in den letzten Jahren sind kontinuierlich angestiegen: 1995: 3667, 1996: 6428, 1997: 7776, 1998: 9802
- Immer mehr Straftatbestände wurden als Grund für eine Telekommunikationsüberwachung in § 100 a der Strafprozessordnung (StPO) einbezogen - der Katalog wurde seit Einführung 11 mal erweitert und damit bis heute nahezu verdoppelt. Neue Erweiterungen sind im Gespräch.
- Die Telekommunikationsanbieter werden verpflichtet, technische Einrichtungen zur Umsetzung der Überwachungsanordnungen zu installieren und Kundendateien für Abfragen durch die Sicherheitsbehörden vorzuhalten zur Feststellung, mit welchen Anbietern verdächtige Personen einen Vertrag haben. Diese Verpflichtung wurde auch auf die Anbieter nicht gewerblicher Netze ausgedehnt und kann nach dem Gesetzeswortlaut auch Hotels, Betriebe, Behörden oder möglicherweise sogar Krankenhäuser betreffen.
- Ein europäischer Anforderungskatalog für Überwachungsmöglichkeiten unter dem Namen "ENFOPOL", befasst sich u. a. mit der Frage, welchen Anforderungen die Netzbetreiber bzw. Diensteanbieter genügen müssen, damit die auf der Grundlage nationaler Ermächtigungsgrundlagen zulässige Telekommunikationsüberwachung technisch durchführbar ist. Die G8-Staaten haben noch weitergehende Beschlüsse gefasst.

Forderungen zur Gewährleistung der freien Telekommunikation

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits 1996 ein Positionspapier erarbeitet. Vor diesem Hintergrund fordert die Konferenz:

- Freie Telekommunikation ist unabdingbar für eine freiheitliche demokratische Kommunikationsgesellschaft. Sie wird durch das Fernmeldegeheimnis geschützt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichts zu den verdachtslosen Abhörmaßnahmen des BND (BVerfG, Urt. v. 14.7.1999, 1 BvR 2226/94 u. a.) auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird. Die Geltung des Fernmeldegeheimnisses ist deshalb auch für den Bereich der Tele- und Mediendienste ausdrücklich klarzustellen.
- Notwendig ist eine bürgerrechtsfreundliche technische Infrastruktur nach dem Grundsatz der Datenvermeidung und dem Datensparsamkeitsprinzip. Dabei ist der Einsatz datenschutzfreundlicher Technologien besonders zu fördern. Anonyme und pseudonyme Nutzungsmöglichkeiten

müssen nach dem Vorbild des Teledienstedatenschutzgesetzes als Pflichtangebote vorgehalten werden. Die Nutzung dieser Angebote darf nicht von der Speicherung von Bestandsdaten abhängig gemacht werden. Eine Vorratshaltung von Daten Unverdächtiger über den Betriebszweck hinaus zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer zukünftiger Straftaten ist als Überwachung auf Vorrat abzulehnen.

- Notwendig ist deshalb ein zusammenfassendes, in sich schlüssiges System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf eine unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt.
- Als Grundlage hierfür ist eine Evaluierung der bestehenden Eingriffsregelungen nach objektiven, nicht zielorientierten Maßstäben vorzunehmen hinsichtlich Effektivität auf der einen und Eingriffsumfang auf der anderen Seite. Eine gesetzliche Berichtspflicht über Anlass, Verlauf, Ergebnisse und Anzahl der Betroffenen ist auch für Telekommunikationsüberwachungen einzuführen. Dass auch Unverdächtige von Abhör- und Kontrollmaßnahmen betroffen sein können, ist dabei besonders zu berücksichtigen.
- Der aus der Frühzeit der analogen Fernsprechtechnik stammende § 12 Fernmeldeanlagengesetz, der die Herausgabe von Verbindungsdaten vergangener, nach bestrittener Rechtsprechung sogar zukünftiger Telekommunikationsvorgänge ohne Beschränkung auf schwerere Straftaten ermöglicht, muss wegen der erheblich höheren Aussagefähigkeit der digitalen Verbindungsdaten und des damit verbundenen Eingriffs in das Fernmeldegeheimnis zügig durch eine weniger weit reichende Regelung in der StPO ersetzt werden.
- Die Anforderungen aus dem bereits zitierten Urteil des Bundesverfassungsgerichts zur Telekommunikationsüberwachung sind unverzüglich umzusetzen.
- Die Ausweitung der Mitwirkungspflichten bei Überwachungsmaßnahmen auf Nebenstelenanlagen in Hotels, Krankenhäuser oder Betrieben wäre unverhältnismäßig. Es muss deshalb verbindlich klargestellt werden, dass die Betreiber dieser Nebenstellenanlagen nicht zur Bereitstellung entsprechender technischer Einrichtungen verpflichtet werden. Das Eckpunktepapier des Bundesministeriums für Wirtschaft und Technologie, das als Grundlage für einen Entwurf der Telekommunikations-Überwachungverordnung dient und nach verschiedenen Gruppen von Betreibern differenziert, ist dazu ein erster Schritt. Auch muss möglichst durch eine Gesetzesänderung verhindert werden, dass die Verpflichtung, Kundendateien zu führen, auch für die o. g. Nebenstellenanlagen gilt. Darüber hinaus dürfen Anbieter von Guthabenkarten zur Mobiltelefonie

nicht dazu verpflichtet werden, Identifikationsdaten ihrer Kunden, die sie für betriebliche Zwecke nicht benötigen, ausschließlich für Zwecke der Strafverfolgungsbehörden und der Nachrichtendienste zu erheben und zum Abruf bereitzuhalten.

- Die Beachtung des Fernmeldegeheimnisses erfordert zwingend die Verschlüsselung von elektronischen Mitteilungen in offenen Netzen. Das Eckpunktepapier der Bundesregierung zur deutschen Kryptopolitik, das eine Kryptoregulierung ablehnt, ist ein wichtiger Schritt in die richtige Richtung. Gewerbliche Telekommunikationsdienstleister sollten gesetzlich verpflichtet werden, die Möglichkeit der verschlüsselten Kommunikation kostenlos zu unterstützen.
- Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen, wie Ärztinnen und Ärzte, Anwältinnen und Anwälte, Psychologinnen und Psychologen, bedürfen besonders im Interesse ihrer Klientel eines umfassenden Schutzes ihrer Telekommunikation.
- Straftaten gegen den Schutz der Privatsphäre ist wirksamer entgegenzutreten. Notwendig sind z. B. die Prüfung eines Verbots des freien Verkaufs von Abhörtechnik, eine Verbesserung der Strafverfolgung im Bereich illegaler Abhörmaßnahmen und eine Verschärfung des strafrechtlichen Schutzes des Fernmeldegeheimnisses.

Anlage 15 **Data Warehouse**, **Data Mining und Datenschutz**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000

Mit der ständig zunehmenden Leistungsfähigkeit der Informations- und Kommunikationstechnik wächst die Menge gespeicherter personenbezogener Daten in Wirtschaft und Verwaltung weiter an. Zunehmend kommen automatisierte Verfahren zum Einsatz, die das gesammelte Datenmaterial effektiv verwalten und analysieren. Im "Data Warehouse" werden alle verwendbaren Daten in einem einheitlichen Datenpool losgelöst von ihrer ursprünglichen Verwendung zusammengeführt. "Data Mining" bietet Werkzeuge, die die scheinbar zusammenhanglosen Daten nach noch nicht bekannten, wissenswerten Zusammenhängen durchsuchen, Daten aufspüren, kombinieren und neue Informationen zur Verfügung stellen.

Diese Entwicklung schafft neben Vorteilen neue Gefahren und Risiken für das Grundrecht auf informationelle Selbstbestimmung und für den Schutz der Privatheit: Persönlichkeitsprofile, automatisierte Vorhersagen von Verhaltens- und Handlungsweisen, Manipulationsmöglichkeiten und zu lange Speicherung sind befürchtete Gefahren.

Die Konferenz der Datenschutzbeauftragten weist auf Folgendes hin:

- Nach dem grundrechtlichen Gebot der Zweckbindung dürfen personenbezogene Daten nur im Rahmen der gesetzlich zugelassenen Zwecke oder der gegenseitigen Vereinbarungen verwendet werden. Eine personenbezogene Speicherung in einem allgemein verwendbaren Data Warehouse entfernt sich vom ursprünglichen Verwendungszweck und stellt eine Speicherung auf Vorrat ohne Zweckbindung dar. Personenbezogene Daten, die bei der öffentlichen Verwaltung vorhanden sind, sind in ihrer Zweckbestimmung grundrechtlich geschützt und dürfen nicht für unbestimmte Zwecke in einem "Daten-Lagerhaus" gesammelt werden.
- Eine Zweckänderung ist nur mit Einwilligung der Betroffenen zulässig, nachdem diese über die Tragweite der Einwilligung aufgeklärt worden ist. Eine Einwilligung in unbestimmte und zeitlich unbegrenzte Zweckänderungen ist deswegen unwirksam.
- Gestaltung und Auswahl von Datenverarbeitungs-Systemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Anonyme und pseudonyme Verfahren sind datenschutzrechtlich unbedenklich.
- Verfahren sind so zu gestalten, dass die Betroffenen hinreichend unterrichtet werden, damit sie jederzeit die Risiken abschätzen und ihre Rechte wahrnehmen können. Sie haben insbesondere das Recht, eine erteilte Einwilligung jederzeit zurückzuziehen.
- Die gesetzlichen Speicherfristen, nach deren Ablauf die Daten zwingend archiviert oder gelöscht werden müssen, sind strikt zu beachten. Deswegen ist die Einrichtung von permanenten "Daten-Lagerhäusern" rechtswidrig.
- Die Europäische Datenschutzrichtlinie spricht grundsätzlich jeder Person das Recht zu, keiner belastenden automatisierten Einzelentscheidung unterworfen zu werden (Art. 15). "Data Mining" ist ein Instrument, das für solche Entscheidungen herangezogen werden kann.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ruft die Hersteller und Anwender von "Data Warehouse"- und "Data Mining"-Verfahren dazu auf, solchen Programmen den Vorzug zu geben, die unter Einsatz von datenschutzfreundlichen Technologien die Speicherung von personenbezogenen Daten durch Anonymisierung oder Pseudonymisierung vermeiden.

Anlage 16 **Konsequenzen aus dem Urteil des Bundesverfassungsgerichts zu den Abhörmaßnahmen des BND**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000

Das Bundesverfassungsgericht hat für die Verwendung von Daten, die aus der Fernmeldeüberwachung gewonnen wurden, deutliche Schranken gezogen, die weit über den Gegenstand des Verfahrens hinaus bedeutsam sind.

Das Gericht betont die Bedeutung des Fernmeldegeheimnisses zur Aufrechterhaltung einer freien Telekommunikation, die eine Grundvoraussetzung der Informationsgesellschaft darstellt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichtes zu den verdachtslosen Abhörmaßnahmen des BND auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird (Telefon, E-Mail, Telefax, Internet-Abrufe o.ä.).

Die Anforderungen des Urteils müssen auch Konsequenzen für Fallgestaltungen, bei denen personenbezogene Daten durch Maßnahmen erlangt werden, die in ihrer Art und Schwere einer Beschränkung des Fernmeldegeheimnisses gleichkommen, insbesondere etwa bei einer Erhebung durch Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes mit dem Einsatz technischer Mittel.

Die Anforderungen aus dem Urteil sind unverzüglich umzusetzen:

- Zur Sicherung der Zweckbindung der erlangten Daten und für die Kontrolle ihrer Verwendung muss ihre Herkunft aus Eingriffen in das Fernmeldegeheimnis oder vergleichbaren Eingriffen durch eine entsprechende Kennzeichnung nach der Erfassung auch bei den Übermittlungsempfängern erkennbar bleiben.
- Die erlangten Daten müssen bei allen speichernden Stellen unverzüglich gelöscht werden, wenn sie nicht mehr erforderlich sind - es sei denn, der Rechtsschutz der Betroffenen würde dadurch verkürzt. Die Praxis von Verfassungsschutzämtern, nicht (mehr) erforderliche Daten, wenn sie sich in Unterlagen befinden, nicht zu schwärzen, kann - zumindest bei Daten, die durch Eingriffe in das Fernmeldegeheimnis oder vergleichbare Eingriffe erlangt wurden - nicht mehr aufrechterhalten werden. Um die Notwendigkeit einer späteren Schwärzung zu vermeiden, sollten bereichsspezifischen Vernichtungsregelungen bereits bei der Aktenführung Rechnung getragen werden.
- Die Vernichtungspflicht ist im Licht von Art. 19 Abs. 4 GG zu verstehen. Danach sind Maßnahmen unzulässig, die darauf abzielen oder geeignet sind, den Rechtsschutz der Betroffenen zu vereiteln. Eine Löschung oder Vernichtung ist nach einem Auskunftsantrag bei allen personenbezoge-

nen Daten unzulässig. Zudem sind personenbezogene Daten, die durch die o.g. Maßnahmen erlangt wurden, nach einer Unterrichtung der Betroffenen für einen angemessenen Zeitraum - ausschließlich zum Zweck der Sicherung des Rechtsschutzes - aufzubewahren.

- Überwachte Personen müssen von Eingriffen unterrichtet werden, sobald dadurch der Zweck der Maßnahme nicht mehr gefährdet wird; dies gilt auch für weitere Betroffene, es sei denn, überwiegende schutzwürdige Belange der überwachten Person stehen dem entgegen (Schutz vor unnötiger Bloßstellung).
- Wie bei Eingriffen in das Fernmeldegeheimnis ist dies auch bei anderen verdeckten Maßnahmen Voraussetzung dafür, dass die Betroffenen von den ihnen zustehenden Rechten Gebrauch machen können, und daher von Art. 19 Abs. 4 GG geboten. Speicherfristen können die Unterrichtungspflicht nicht beseitigen, irrelevante Daten sind umgehend zu löschen.
- Damit sind Regelungen z.B. in Landesverfassungsschutz- und Polizeigesetzen nicht zu vereinbaren, wonach eine Unterrichtung der Betroffenen über Datenerhebungen, die in ihrer Art und Schwere einem Eingriff in das Fernmeldegeheimnis gleichkommen, unterbleibt, wenn sich auch nach fünf Jahren nicht abschließend beurteilen lässt, ob eine Gefährdung des Zweckes des Eingriffes ausgeschlossen werden kann.
- Zusätzlich zur unbefristeten Benachrichtigungspflicht ist eine Mitteilung an die Datenschutzkontrollstelle für den Fall vorzusehen, dass die Unterrichtung der Betroffenen länger als fünf Jahre zurückgestellt wird.
- Der Umgang des Verfassungsschutzes mit personenbezogenen Daten, die in Durchbrechung des Fernmeldegeheimnisses erhoben worden sind, ist durch eine unabhängige Datenschutzkontrollstelle lückenlos zu überprüfen.
- Eine Kontrolllücke bei personenbezogenen Daten, die durch G 10-Maßnahmen erlangt wurden, wäre verfassungswidrig. Das Bundesverfassungsgericht hat hervorgehoben, dass Art. 10 GG eine umfassende Kontrolle durch unabhängige und an keine Weisung gebundene staatliche Organe und Hilfsorgane gebietet.
- Die Kontrolle muss sich auf den gesamten Prozess der Erfassung und Verwertung der Daten einschließlich der Benachrichtigung - bei Datenübermittlungen auch bei den Datenempfängern - erstrecken.
- Der Gesetzgeber sollte festlegen, dass die Übermittlung der Daten, die Prüfung der Erforderlichkeit weiterer Speicherung sowie die Durchführung der Vernichtung und Löschung der Daten aus G 10-Maßnahmen zu protokollieren sind.

- Für eine effektive Kontrolle sind die zuständigen Stellen personell und sachlich angemessen auszustatten.
- Die Ausführungsgesetze zum G 10 müssen hinsichtlich der Kontrolle eindeutig sein. Es ist klarzustellen, inwieweit die G 10-Kommissionen auch für die Kontrolle der weitergehenden Datenverarbeitung zuständig sind oder inwieweit die Kontrolle von den Datenschutzbeauftragten wahrzunehmen ist.

Anlage 17 **Strafverfahrensänderungsgesetz 1999 (StVÄG 1999)**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen es, dass mit dem Entwurf für ein Strafverfahrensänderungsgesetz 1999 die Strafprozessordnung endlich die seit fast zwei Jahrzehnten überfälligen datenschutzrechtlichen Regelungen erhalten soll. Sie stellen jedoch fest, dass der nunmehr vorliegende Gesetzesbeschluss des Bundestages nicht alle wichtigen Forderungen des Datenschutzes erfüllt.

Darüber hinaus will der Bundesrat das Datenschutzniveau weiter absenken und hat auch zu diesem Zweck den Vermittlungsausschuss angerufen. Zu kritisieren ist, dass

- Zeuginnen und Zeugen auch bei Straftaten ohne erhebliche Bedeutung durch Öffentlichkeitsfahndung im Fernsehen oder Internet gesucht werden können,
- Zweckbindungen präventivpolizeilicher Daten, darunter auch der Erkenntnisse aus verdeckten Datenerhebungsmaßnahmen, wie z. B. einem Großen Lauschangriff oder einem Einsatz verdeckter Ermittler, völlig aufgehoben werden, so dass sie uneingeschränkt zur Strafverfolgung genutzt werden können,
- umgekehrt aber auch Informationen aus Strafverfahren über die Gefahrenabwehr hinaus uneingeschränkt zur Gefahrenvorsorge genutzt werden können,
- nicht am Verfahren beteiligte Dritte schon bei "berechtigtem Interesse" Einsicht in Strafverfahrensakten bekommen können.

Die Datenschutzbeauftragten des Bundes und der Länder sehen den verfassungsrechtlich gebotenen Ausgleich zwischen Persönlichkeitsschutz und Interessen der Strafverfolgungsbehörden nicht mehr als gewährleistet an, falls die Vorschläge des Bundesrates Eingang in die Strafprozessordnung finden sollten. Die Datenschutzbeauftragten fordern daher den Vermittlungsausschuss auf, die Änderungsanträge zurückzuweisen. Stattdessen sind Regelungen in der Strafprozessordnung vorzusehen, die geeignet sind,

bei einer effektiven Strafverfolgung die Persönlichkeitsrechte der Betroffenen angemessen zu gewährleisten

Anlage 18 **Unzulässiger Speicherungsumfang in "INPOL-neu" geplant**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000

Das Bundeskriminalamt und die Polizeien der Bundesländer konzipieren seit geraumer Zeit unter der Bezeichnung "INPOL-neu" eine Fortentwicklung des gemeinsamen Informationssystems. Inzwischen steht der Beginn der schrittweisen Einführung des neuen Datenaustauschsystems kurz bevor.

Das Informationssystem INPOL wirft in vielfacher Hinsicht datenschutzrechtliche Probleme auf. Die Datenschutzbeauftragten des Bundes und der Länder haben mehrfach aus konkretem Anlass darauf hingewiesen, dass nicht jede mit den heutigen technischen Möglichkeiten realisierbare oder mit polizeifachlicher Erforderlichkeit begründete Verarbeitung personenbezogener Daten zulässig ist. Bereits bei der Konzeption des INPOL-Systems muss vielmehr dafür Sorge getragen werden, dass in das Recht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung nur soweit eingegriffen wird, wie dies im Rahmen der Erforderlichkeit für die polizeiliche Aufgabenerfüllung durch Rechtsvorschriften erlaubt wird.

Es besteht jedoch Grund zu der Sorge, dass es bei der Neugestaltung des INPOL-Systems zu falschen Weichenstellungen mit der Folge unzulässiger Verarbeitung personenbezogener Daten kommt. Die zu befürchtende Fehlentwicklung liegt darin, dass das Bundeskriminalamt und die Landeskriminalämter planen, künftig im Bundes-Kriminalaktennachweis (KAN) die "gesamte kriminelle Karriere" jeder Person abzubilden, die aus Anlass eines INPOL-relevanten Delikts erfasst ist. Es sollen in diesen Fällen auch Daten über solche Straftaten gespeichert und zum Abruf bereit gehalten werden, die weder von länderübergreifender oder internationaler noch von besonderer Bedeutung sind.

§ 2 Abs. 1 BKAG beschränkt die Zuständigkeit des BKA (als Zentralstelle des polizeilichen Informationssystems) sowohl im präventiven als auch im repressiven Bereich auf "Straftaten mit länderübergreifender, internationaler oder erheblichen Bedeutung". Der Wortlaut ist eindeutig. Anknüpfungspunkt und Gegenstand der Einteilung in INPOL-relevante Informationen einerseits und INPOL-irrelevante Informationen andererseits sind die "Straftaten", nicht die einzelne Person und auch nicht das "Gesamtbild einer Person". Der Gesetzeswortlaut bildet die Grenze der Auslegung; eine über den Wortsinn hinausgehende Anwendung verstößt gegen das Gesetz. Daher ist es unzulässig, die Frage der INPOL-Relevanz unabhängig von der konkreten ein-

zelnen Straftat zu beurteilen. Vielmehr dürfen im Bundes-KAN nur Informationen zu solchen Straftaten verarbeitet werden, die im Einzelfall die in § 2 Abs. 1 BKAG aufgestellte Bedeutungsschwelle überschreiten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern das Bundesinnenministerium und die Innenministerien der Länder auf, von der geschilderten KAN-Erweiterung abzusehen.

Anlage 19 **Auftragsdatenverarbeitung durch das Bundeskriminalamt**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 10. Oktober 2000

Im Rahmen der Neukonzeption des polizeilichen Informationssystems INPOL ist geplant, neben bundesweit verfügbaren Verbunddaten auch Landesdatenbestände im Wege der Auftragsdatenverarbeitung logisch getrennt in der INPOL-Datenbank zu speichern. Zudem sollen aufgrund bilateraler Absprachen landesspezifische Informationen in bestimmtem Umfang gespeichert werden können und ebenso gegenseitige Zugriffe einzelner Länder auf die Datenbestände ermöglicht werden.

§ 2 Abs. 5 des Bundeskriminalamtgesetzes lässt grundsätzlich eine Unterstützung der Länder bei deren Datenverarbeitung auf Ersuchen, also in Einzelfällen, zu. Diese Vorschrift kann auch herangezogen werden, wenn aufgrund besonderer Dringlichkeit, wie gegenwärtig bei der Realisierung von INPOL-neu, eine zeitlich befristete Auftragsdatenverarbeitung von Landesdaten geplant ist. Hierzu sind Ende vergangenen Jahres entsprechende Beschlüsse des Arbeitskreises und der Innenministerkonferenz gefasst worden.

Diese Entwicklung birgt aus der Sicht der Datenschutzbeauftragten die Gefahr, dass weitere Beschlüsse folgen werden, die die dauerhafte Speicherung von Landesdaten beim BKA begründen; bereits jetzt sind Tendenzen deutlich, die zentralisierte Speicherung der Daten auch zur Erleichterung der gegenseitigen Zugriffe auf Landesdaten zu nutzen.

Die Notwendigkeit der zentralen Datenspeicherung beim Bundeskriminalamt wird im Wesentlichen mit Kosten- und Zeitargumenten begründet. Diese sind jedoch aus datenschutzrechtlicher Sicht nicht geeignet, eine Erweiterung der zentralen Datenverarbeitung beim Bundeskriminalamt zu begründen.

Die dauerhafte zentrale Datenhaltung beim BKA würde die informationelle Trennung von Landesdaten und Verbunddaten aufweichen; die in § 2 Abs. 1 BKA-Gesetz statuierte Schwelle, dass nur Daten über Straftaten von län-

derübergreifender, internationaler oder sonst erheblicher Bedeutung beim BKA verarbeitet werden dürfen, würde schleichend umgangen.

Eine dauerhafte zentrale Landesdatenhaltung beim Bundeskriminalamt beinhaltet eine neue, bei der augenblicklichen Rechtslage unakzeptable Qualität polizeilicher Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren an die Innenminister/-senatoren von Bund und Ländern, an den bisherigen Beschlüssen festzuhalten und die Polizeien der Länder, wie ursprünglich geplant, aufzufordern, unverzüglich eigene Datenverarbeitungsverfahren zu entwickeln. Bis zur Realisierung dieser Verfahren könnte allenfalls eine übergangsweise Lösung als Auftragsdatenverarbeitung unter Wahrung datenschutzrechtlicher Anforderungen ermöglicht werden. Daneben steht das Angebot des Bundeskriminalamtes, kostenlos Software von INPOL-neu zur Verfügung zu stellen. Diese Lösung würde auch das vorgetragene Kostenargument entkräften.

Anlage 20 **Effektive parlamentarische Kontrolle von Lauschangriffen durch aussagekräftige jährliche Berichte der Bundesregierung**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000

Die Bundesregierung hat den Bundestag jährlich über die nach Art. 13 Abs. 3 GG zur Strafverfolgung eingesetzten "Großen Lauschangriffe" zu unterrichten. § 100e StPO konkretisiert die Berichtspflicht dahingehend, dass die Bundesregierung aufgrund von Mitteilungen der Staatsanwaltschaften der Länder den Bundestag über Anlass, Umfang, Dauer, Ergebnis und Kosten der Maßnahmen zu unterrichten hat.

Diese Berichte sollen eine laufende parlamentarische Kontrolle dieser mit intensiven Grundrechtseingriffen verbundenen Maßnahmen ermöglichen. Der Bundestag soll aufgrund der Berichte in die Lage versetzt werden, die Angemessenheit und Eignung der Maßnahme zu überprüfen.

Diesen Anforderungen wird der erste von der Bundesregierung vorgelegte Bericht nicht in vollem Umfang gerecht. So wurde nur die Gesamtzahl der von der Anordnung Betroffenen erfasst, wobei zwischen Beschuldigten und nicht beschuldigten Wohnungsinhabern unterschieden wird.

Nach § 100e Abs. 1 STPO muss über den Umfang der Maßnahme berichtet werden. Hierzu zählt die Angabe über die Anzahl aller von der Maßnahme betroffenen Personen, nicht nur der in der gerichtlichen Anordnung genannten. Von dem "Großen Lauschangriff" ist jeder betroffen, dessen gesprochenes Wort in der Wohnung abgehört wird. Er greift auch in die grund-

rechtlich geschützten Rechte der am Verfahren Unbeteiligten, wie z.B. unverdächtige Familienangehörige, Bekannte, Besucherinnen und Besucher sowie sonstige Personen, die nicht selbst Wohnungsinhaber sind, ein. Dem wollte der Gesetzgeber mit der Einführung der Berichtspflicht Rechnung tragen.

Die Beschränkung der Berichtspflicht auf Wohnungsinhaber und Beschuldigte gibt nicht den wirklichen Umfang der von der Maßnahme betroffenen Personen wieder. Somit erfüllt sie den Zweck der im Grundgesetz vorgesehenen Berichtspflicht nicht.

Darüber hinaus wäre es wünschenswert, wenn - wie in den "Wire-tap-Reports" der USA - die Anzahl der abgehörten Gespräche und die Anzahl der Gespräche, die mit dem Ermittlungsverfahren in Zusammenhang stehen, die Art der betroffenen Räume (Geschäftsräume, Wohnung, Restaurant etc.), die Anzahl und Dauer der angeordneten Verlängerungen der Maßnahme, die Zahl der Verhaftungen, Anklageerhebungen und Verurteilungen, zu denen die Maßnahme beigetragen hat, angegeben werden.

Die Länder haben nach Art. 13 Abs. 6 Satz 3 GG eine gleichwertige parlamentarische Kontrolle zu gewährleisten. Die oben genannten Forderungen gelten deshalb gleichermaßen bzw. in entsprechender Weise für die den Landesparlamenten vorzulegenden jährlichen Berichte über die nach § 100c Abs. 1 Nr. 3 StPO durchgeführten Maßnahmen bzw. über die von der Polizei zur Gefahrenabwehr veranlassten "Großen Lauschangriffe".

Anlage 21 **Vom Bürgerbüro zum Internet - Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000

Bei der Modernisierung der öffentlichen Verwaltung soll insbesondere die Dienstleistungs- und Serviceorientierung verbessert werden. Dazu sollen unter anderem Dienstleistungen in multifunktionalen Servicecentern (Bürgeramt, Bürgerbüro, Bürgerladen, Kundencenter) gebündelt und die Möglichkeiten der modernen Informations- und Kommunikations-Technik intensiver genutzt werden (Information, Kommunikation und Transaktion über das Internet, Einrichtung von Call-Centern).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt alle Bemühungen, den Kontakt von Bürgerinnen und Bürgern mit den Verwaltungen schneller, einfacher, effektiver und insbesondere transparenter zu machen. Die Datenschutzbeauftragten erklären daher ihre ausdrückliche Bereitschaft, solche Entwicklungsprozesse konstruktiv zu begleiten.

Es ist aber unerlässlich, dass bei allen Lösungen eine sichere und vertrauliche Kommunikation zwischen Verwaltung und Bürgern sowie ein angemessener Schutz personenbezogener Daten gewährleistet wird. Nur Serviceangebote, die dem Recht auf informationelle Selbstbestimmung gerecht werden, nützen letztlich sowohl Bürgerinnen und Bürgern als auch der Verwaltung selbst.

Eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet deshalb Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung. Diese Empfehlungen sollen den Verwaltungen helfen, bei der Verbesserung ihrer Dienstleistungs- und Serviceorientierung den Forderungen nach Datenschutz und Datensicherheit gerecht zu werden. Diese Empfehlungen werden demnächst veröffentlicht und entsprechend der rechtlichen und technischen Entwicklung fortgeschrieben.

Anlage 22 **Novellierung des BDSG**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an Bundestag und Bundesrat, das Gesetzgebungsverfahren eines novellierten Bundesdatenschutzgesetzes zügig und ohne Abstriche zum Abschluss zu bringen. Damit wird die längst überfällige Anpassung des deutschen Datenschutzrechts an die Vorgaben der EG-Richtlinie vorgenommen. Die Novelle enthält verschiedene innovative Ansätze, insbesondere das Gebot zur Datenvermeidung und Datensparsamkeit bei der Systemgestaltung (Systemdatenschutz - § 3a E-BDSG) und die Einführung des Datenschutzaudit (§ 9a), die von den Datenschutzbeauftragten schon seit langem befürwortet werden.

Sowohl der Systemdatenschutz als auch das Datenschutzaudit werden die Durchsetzung datenschutzfreundlicher Lösungen im Wettbewerb erleichtern und tragen auf diese Weise zur Selbstregulierung des Marktes bei. Das Datenschutzaudit fügt sich in die bewährten Strukturen des betrieblichen Datenschutzes ein und ermöglicht es den Unternehmen, datenschutzkonforme Angebote und Verhaltensweisen nachprüfbar zu dokumentieren und damit einen Wettbewerbsvorsprung zu gewinnen.

Die Konferenz fordert den Bundesrat auf, die Aufnahme des Datenschutzaudit in das BDSG nicht zu blockieren. Sie geht weiter davon aus, dass die angekündigte zweite Stufe der Novellierung des BDSG noch in dieser Legislaturperiode realisiert wird, und erklärt ihre Bereitschaft, hieran konstruktiv mitzuwirken.

Anlage 23 **Datensparsamkeit bei der Rundfunkfinanzierung**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000

Die Finanzierung des öffentlich-rechtlichen Rundfunks ist derzeit Gegenstand öffentlicher Diskussion in der Politik und unter den Rundfunkanstalten selbst. Erörtert wird hierbei auch, ob die Erhebung von Rundfunkgebühren, die an das "Bereithalten eines Rundfunkempfangsgerätes" anknüpfen, im Hinblick auf veränderte Gerätetechniken und bestehende Mängel im Verfahren modifiziert oder durch andere Finanzierungsformen ersetzt bzw. ergänzt werden sollte.

Künftig wird kaum noch überschaubar sein, welche Geräte zum Rundfunkempfang geeignet sind. Über die eigentlichen Fernseh- und Rundfunkgeräte hinaus ist dies bereits heute beispielsweise mit Personalcomputern, die über einen Internetzugang verfügen, oder mit bestimmten Mobiltelefonen möglich. In naher Zukunft werden neue Technologien wie UMTS weitere Empfangsmöglichkeiten eröffnen. Sofern der Besitz derartiger multifunktionaler Geräte zum Kriterium für die Rundfunkgebührenpflicht gemacht wird, würde das zu einer erheblichen Ausweitung von Datenabgleichen führen. Schon das gegenwärtig praktizierte Gebühreneinzugsverfahren erfordert in großem Umfang die Verarbeitung personenbezogener Daten. Nach den Angaben der Rundfunkanstalten meldet ein signifikanter Teil der Rundfunkteilnehmerinnen und -teilnehmer trotz der Verpflichtung hierzu seine Geräte nicht an. Um möglichst alle Gebührenpflichtigen zu erfassen, nutzen die Rundfunkanstalten Daten aus dem Melderegister, vom privaten Adresshandel und setzen vor Ort Rundfunkgebührenbeauftragte ein, die einzelne Haushalte aufsuchen. Damit wird in unverhältnismäßiger Weise in das Recht auf informationelle Selbstbestimmung vieler gesetzestreuer Bürgerinnen und Bürger eingegriffen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesländer auf, einer Neuordnung ein Modell zu Grunde zu legen, das sich stärker als das bestehende System der Rundfunkfinanzierung an den Prinzipien der Datenvermeidung, Datensparsamkeit und Dezentralisierung orientiert. Nach ihrer Überzeugung lässt sich die verfassungsrechtlich gebotene Staatsferne und Funktionsfähigkeit des öffentlich-rechtlichen Rundfunks auch mit anderen, das Recht auf informationelle Selbstbestimmung weniger stark einschränkenden Finanzierungsmodellen als dem derzeit praktizierten gewährleisten.

Anlage 24 **Datenschutzrechtliche Konsequenzen aus der Entschlüsselung des menschlichen Genoms**

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000

Bei der Entschlüsselung des menschlichen Genoms sind in den letzten Monaten wohl entscheidende Durchbrüche gelungen. Für mehr als 20, oft vererbliche Krankheiten sind bereits Gentests zu erwerben, mit denen in Labors analysiert werden kann, ob eine Erkrankung vorliegt bzw. in welchem Umfang ein Erkrankungsrisiko besteht. Viele dieser Krankheiten sind allerdings bisher nicht heil- oder behandelbar.

Gentechnische Untersuchungen beim Menschen eröffnen den Zugang zu höchstpersönlichen und hochsensiblen Informationen in einem Maße, das die Intensität bisheriger personenbezogener Informationen ganz erheblich übersteigt. Durch den genetischen Einblick in den Kernbereich der Privatsphäre, etwa in Gesundheitsdisposition, Anlagen der Persönlichkeitsstruktur oder den voraussichtlichen Lebensverlauf, entsteht eine ganz neue Qualität des Wissens und des Offenlegens von persönlichsten Daten. Sowohl für die Betroffenen als auch für dritte Personen, insbesondere Familienangehörige, ist es von entscheidender Bedeutung, ob und inwieweit sie selbst und wer außer ihnen von den Ergebnissen Kenntnis bekommt. Davor steht die Frage, ob und aus welchen Anlässen überhaupt genetische Untersuchungen am Menschen vorgenommen werden dürfen. Zur informationellen Selbstbestimmung gehört auch das Recht auf Nichtwissen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass für die Zulässigkeit gentechnischer Untersuchungen beim Menschen und für den Umgang mit den dabei gewonnenen Informationen sehr schnell klare und verbindliche Prinzipien entwickelt werden, um auch die informationelle Selbstbestimmung in diesem Kernbereich zu sichern und zugleich eine "genetische Diskriminierung" bei der Gewinnung oder Verwendung genetischer Informationen, etwa im Arbeitsverhältnis oder beim Abschluss von Versicherungsverträgen zu verhindern. Auf der Grundlage dieser und in der "Entschließung über Genomanalyse und informationelle Selbstbestimmung" vom 26. Oktober 1989 formulierten Grundsätze wird die Konferenz an der Ausgestaltung mitwirken.

Die Datenschutzbeauftragten erinnern an ihre Grundsätze aus der Entschließung von 1989 bezüglich der Genomanalyse:

1. Die Genomanalyse darf grundsätzlich nur auf freiwilliger Basis nach umfassender Aufklärung der Betroffenen vorgenommen werden; ausgenommen sind Straf- und Abstammungsverfahren.

2. Die jederzeit widerrufliche Einwilligung muss sich auch auf die weitere Verwendung der gentechnischen Informationen erstrecken. Im Falle eines Widerrufs sind die gewonnnen Informationen zu löschen oder an den Betroffenen herauszugeben.

3. Jede Genomanalyse muss zweckorientiert vorgenommen werden. Es ist diejenige genomanalytische Methode zu wählen, die keine oder die geringste Menge an Überschussinformationen bringt. Überschussinformationen sind unverzüglich zu vernichten.

4. Es ist zu prüfen, inwieweit genomanalytische Untersuchungsmethoden einer staatlichen Zulassung bedürfen. Für DNA-Sonden ist dies jedenfalls zu bejahen.

5. Die Genomanalyse im gerichtlichen Verfahren muss auf die reine Identitätsfeststellung beschränkt werden; es dürfen keine genomanalytischen Methoden angewandt werden, die Überschussinformationen zur Person liefern. Die Nutzung der Genomanalyse im Strafverfahren setzt eine normenklare gesetzliche Ermächtigung voraus. Präzise Regelungen müssen u.a. sicherstellen, dass genomanalytische Befunde einer strengen Zweckbindung unterworfen werden.

6. Im Arbeitsverhältnis sind die Anordnung von Genomanalysen oder die Verwendung ihrer Ergebnisse grundsätzlich zu verbieten. Ausnahmen bedürfen der gesetzlichen Regelung. Eine bloße Einwilligung des Arbeitnehmers ist wegen der faktischen Zwangssituation, der er im Arbeitsleben häufig unterliegt, nicht ausreichend.

7. Genomanalysen im Versicherungswesen sind grundsätzlich nicht erforderlich und mit dem Prinzip der Versicherungen, Risiken abzudecken und nicht auszuschließen, unvereinbar. Dies sollte durch eine Klarstellung im Versicherungsvertragsgesetz deutlich gemacht werden.

8. Im Rahmen der pränatalen Diagnostik dürfen nur Informationen über das Vorhandensein oder Fehlen von Erbanlagen erhoben werden, bei denen eine Schädigung heilbar ist oder die zu einer so schwerwiegenden Gesundheitsschädigung des Kindes führen würden, dass ein Schwangerschaftsabbruch straffrei bliebe.

   Reihenuntersuchungen an Neugeborenen dürfen sich nur auf solche Erbkrankheiten erstrecken, die bei frühzeitiger Erkennung eines genetischen Defekts geheilt oder zumindest spürbar therapeutisch begleitet werden können.

   Die Eltern müssen nach umfassender fachkundiger Beratung in voller Freiheit über die Anwendung genomanalytischer Methoden entscheiden

können. Jegliche Beeinflussung, insbesondere jeder individuelle und gesellschaftliche Druck, muss vermieden werden.

Die informationelle Selbstbestimmung Dritter, zu der auch das Recht auf Nichtwissen gehört, muss berücksichtigt werden. Demnächst werden nicht nur - wie bisher - Gensequenzen aufgedeckt und verglichen, sondern auch die mit dem Genom verbundenen Wirkungszusammenhänge für die menschliche Gesundheit und für die Persönlichkeitsstruktur entschlüsselt werden können.

Abkürzungsverzeichnis

ADV	Automatisierte Datenverarbeitung
AO	Abgabenordnung
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BGS	Bundesgrenzschutz
BIOS	Basis-Betriebssystem eines PC als Voraussetzung für den technischen Zugriff auf die einzelnen Komponenten (braucht nicht installiert zu werden, da es zur Grundausstattung gehört)
BKA	Bundeskriminalamt
BND	Bundesnachrichtendienst
BSI	Bundesamt für die Sicherheit in der Informationstechnik
BuStra	Bußgeld- und Strafsachenstelle
BVB	Besondere Vertragsbedingungen zur Regelung der Beziehungen der öffentlichen Hand mit privaten Auftragnehmern (z.B. Miete, Kauf, Wartung, Pflege usw.)
BVerfG	Bundesverfassungsgericht
DNA	Desoxyribonukleinsäure-Analyse (Molekular genetische Untersuchung)
DV	Datenverarbeitung
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
eMail	Elektronische versandte Post
EPVS	Einheitliches Personalverwaltungssystem
EU	Europäische Union
EVB	Ergänzende Vertragsbedingungen
FAG	Fernmeldeanlagengesetz
GewO	Gewerbeordnung
GEZ	Gebühreneinzugszentrale
GG	Grundgesetz
GGO	Gemeinsame Geschäftsordnung für die Obersten Landesbehörden
GMBl	Gemeinsames Ministerialblatt des Saarlandes
Homepage	Informationsangebot im Internet mit Darstellung des Anbieters
HWK	Handwerkskammer
IfSG	Infektionsschutzgesetz
IHK	Industrie- und Handelskammer
IK-Ausschuss	Ausschuss für Informationstechnologie und Kommunikation
IMK	Konferenz der Innenminister
IT	Informationstechnik
IZ-Steufa	Informationszentrale für den Steuerfahndungsdienst
KAG	Kommunalabgabengesetz

Kfz	Kraftfahrzeug
KZVS	Kassenzahnärztliche Vereinigung Saarland
LfD	Landesbeauftragter für Datenschutz
MBKW	Ministerium für Bildung, Kultur und Wissenschaft
MDK	Medizinischer Dienst der Krankenversicherung
MiFAGS	Ministerium für Frauen, Arbeit, Gesundheit und Soziales
MiStra	Anordnung über Mitteilungen in Strafsachen
NJW	Neue Juristische Wochenschrift
OFD	Oberfinanzdirektion
ÖGDG	Gesetz über den öffentlichen Gesundheitsdienst
OLG	Oberlandesgericht
OWiG	Gesetz über Ordnungswidrigkeiten
PC	Personal-Computer
PGP	Pretty good privacy: International bekanntes Verschlüsselungsverfahren, das mit öffentlichen und privaten Schlüsseln arbeitet
Pkw	Personenkraftwagen
SBG	Saarländisches Beamtengesetz
SDSG	Saarländisches Datenschutzgesetz
SGB	Sozialgesetzbuch
SKHG	Saarländisches Krankenhausgesetz
SLStatG	Saarländisches Statistikgesetz
SPolG	Saarländisches Polizeigesetz
SSL	Secure Socket Layer: gesichertes Übertragungsverfahren im Internet
Steufa	Steuerfahndungsstelle
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVÄG	Strafverfahrensänderungsgesetz
TB	Tätigkeitsbericht
TK	Telekommunikation
TZ	Textziffer
vDSB	Virtuelles Datenschutzbüro
VHS	Volkshochschule
VO	Verordnung
VÜ-RiLi	Richtlinien für die polizeiliche Verkehrsüberwachung
WE-Meldung	Erlass über die Meldung wichtiger Ereignisse

22